11.04.00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

EJU

出願年月日
Date of Application: １９９９年　５月２４日

出願番号
Application Number: 平成１１年特許願第１４３９８８号

出願人
Applicant (s): ソニー株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年　３月１０日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

出証番号　出証特２０００－３０１５８２５

【書類名】　特許願

【整理番号】　9900478304

【提出日】　平成11年 5月24日

【あて先】　特許庁長官　殿

【国際特許分類】　G11B　7/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　浅野　智之

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　大澤　義知

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100067736

【弁理士】

【氏名又は名称】　小池　晃

【選任した代理人】

【識別番号】　100086335

【弁理士】

【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第105966号

【出願日】　平成11年 4月13日

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置

【特許請求の範囲】

【請求項１】　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する送信制御手段とを備えるデータ送信装置と、

伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記インターフェースを介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する受信制御手段とを備えるデータ受信装置と

からなることを特徴とするデータ伝送システム。

【請求項２】　データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行することを特徴とする請求項１記載のデータ伝送システム。

【請求項３】　音楽データを上記第１の伝送モードで伝送し、上記音楽データに関する関連データを第２の伝送モードで伝送することを特徴とする請求項１記載のデータ伝送システム。

【請求項４】　上記データ送信装置とデータ受信装置をＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを介して接続し、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送することを特徴とする請求項１記載のデータ伝送システム。

【請求項５】　データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行することを特徴とする請求項４記載のデータ伝送システム。

【請求項６】　上記データ受信装置側でｍビットの２つの乱数Ｂｎ１，Ｂｎ２を生成してデータ送信装置に送り、

上記データ送信装置側でｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ２と受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、その出力の最上位ｍビットをレスポンスデータＲ２とし、

Ｒ２＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

このレスポンスデータＲ２を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報Ｋｖと受信した乱数Ａｎ１と上記データ送信装置に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)一方向関数Ｈ［］に入力し、その出力の最上位ｍビットをレスポンスデータＲ１とし、

Ｒ１＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

このレスポンスデータＲ１を上記データ送信装置に送り、

上記データ送信装置では、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ１と受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｒ’１＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

その出力の最上位ｍビットを参照データＲ’１とし、この参照データＲ’１が受信したレスポンスデータＲ１と一致した場合に、上記連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｋiso ＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とするとともに、上記連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｋasync＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とし、

上記データ受信装置では、自分が正当であることを示す情報Ｋｖと受信した乱数Ａｎ２と上記データ送信装置に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｒ’２＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットを参照データＲ’２ とし、この参照データＲ’２ が受信したレスポンスデータＲ２と一致した場合に、上記連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｋ’iso ＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵K’iso とするするとともに、上記連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２)を一方向関数Ｈ［］に入力し、

Ｋ’async＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵K’async とする

ことを特徴とする請求項５記載のデータ伝送システム。

【請求項７】　上記データ受信装置側でｍビットの２つの乱数Ｂｎ１，Ｂｎ２を生成してデータ送信装置に送り、

上記データ送信装置側でｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ２と受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向

関数Ｈ［］に入力し、

Ｒ２＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットをレスポンスデータＲ２とし、このレスポンスデータＲ２を上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ１と受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１）を一方向関数Ｈ［］に入力し、

Ｒ’１＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットを参照データＲ’１とするとともに、

Ｋiso＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とし、上記暗号鍵Ｋiso と上記データ受信装置に送った乱数Ａｎ１と受信した乱数Ｂｎ１を連結した連結データ（Ｋiso ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋiso ‖Ａｎ１‖Ｂｎ１）を一方向関数Ｈ［］に入力し、

Ｒ２＝Ｈａｓｈ［Ｋiso‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ２として、このレスポンスデータＲ２を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報Ｋｖと受信した乱数Ａｎ１と上記データ送信装置に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｒ１＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ１とするとともに、

Ｋ’iso＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵Ｋ’isoとし、上記暗号鍵Ｋ’isoと受信した乱数Ａｎ２と上記データ送信装置に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ(Ｋｖ ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｒ’２　＝Ｈ［Ｋ’iso‖Ａｎ２‖Ｂｎ２］msb_p

その出力の最上位ｐビットを参照データＲ’２ とし、上記データ送信装置から送られてきたレスポンスデータＲ２と上記参照Ｒ’２ とを比較して一致した場合に、上記レスポンスデータＲ１を上記データ送信装置に送り、

上記データ送信装置は、上記データ受信装置から送られてきたスポンスデータＲ１と上記参照データＲ’１ とを比較して一致した場合に、上記暗号鍵Ｋiso と上記データ受信装置に送った乱数Ａｎ２と受信した乱数Ｂｎ２を連結した連結データ（Ｋiso ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ（Ｋiso‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｋasync＝Ｈ［Ｋiso ‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とし、

また、上記データ受信装置は、上記暗号鍵Ｋ’isoと受信した乱数Ａｎ２と上記データ送信装置に送った乱数Ｂｎ２を連結した連結データ（Ｋ’iso‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（Ｋ’iso‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｋ’async＝Ｈ［Ｋ’iso‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵Ｋ’async とする

ことを特徴とする請求項５記載のデータ伝送システム。

【請求項８】　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介してデータ伝送を行うデータ伝送方法であって、

伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで伝送し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで伝送する

ことを特徴とするデータ伝送方法。

【請求項９】　データ伝送に先立って、データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する

ことを特徴とする請求項８記載のデータ伝送方法。

【請求項１０】　音楽データを上記第１の伝送モードで伝送し、上記音楽データに関するデータを第２の伝送モードで伝送する

ことを特徴とする請求項８記載のデータ伝送方法。

【請求項１１】　データ送信装置とデータ受信装置との間で、ＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを介して、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送する

ことを特徴とする請求項７記載のデータ伝送方法。

【請求項１２】　データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する

ことを特徴とする請求項１１記載のデータ伝送方法。

【請求項１３】　上記データ受信装置側でｍビットの２つの乱数Ｂｎ１，Ｂｎ２を生成してデータ送信装置に送り、

上記データ送信装置側でｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ２と受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、その出力の最上位ｍビットをレスポンスデータＲ２とし、

Ｒ２＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

このレスポンスデータＲ２を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報Ｋｖと受信した乱数Ａｎ１と上記データ送信装置に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)一方向関数Ｈ［］に入力し、その出力の最上位ｍビットをレスポンスデータＲ１とし、

Ｒ１＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

このレスポンスデータＲ１を上記データ送信装置に送り、

上記データ送信装置では、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ１と受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｒ’１＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

その出力の最上位ｍビットを参照データＲ’１とし、この参照データＲ’１が受信したレスポンスデータＲ１と一致した場合に、上記連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｋiso ＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とするとともに、上記連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｋasync＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とし、

上記データ受信装置では、自分が正当であることを示す情報Ｋｖと受信した乱数Ａｎ２と上記データ送信装置に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｒ’２＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットを参照データＲ’２とし、この参照データＲ’２が受信したレスポンスデータＲ２と一致した場合に、上記連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｋ’iso ＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵Ｋ’iso とするするとともに、上記連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２)を一方向関数Ｈ［］に入力し、

Ｋ’async＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵Ｋ'async とする

ことを特徴とする請求項１２記載のデータ伝送方法。

【請求項１４】　上記データ受信装置側でｍビットの２つの乱数Ｂｎ１，Ｂｎ２を生成してデータ送信装置に送り、

上記データ送信装置側でｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ２と受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｒ２＝Ｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットをレスポンスデータＲ２とし、このレスポンスデータＲ２を上記データ受信装置に送り、

上記データ送信装置は、自分が正当であることを示す情報Ｋｖと上記データ受信装置に送った乱数Ａｎ１と受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１）を一方向関数Ｈ［］に入力し、

Ｒ'１　＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットを参照データＲ'１　とするとともに、

Ｋiso　＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とし、上記暗号鍵Ｋiso と上記データ受信装置に送った乱数Ａｎ１と受信した乱数Ｂｎ１を連結した連結データ（Ｋiso ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋiso ‖Ａｎ１‖Ｂｎ１）を一方向関数Ｈ［］に入力し、

Ｒ２＝Ｈａｓｈ［Ｋiso‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ２として、このレスポンスデータＲ２を上記データ受信装置に送り、

上記データ受信装置は、自分が正当であることを示す情報Ｋｖと受信した乱数

Ａｎ１と上記データ送信装置に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)を一方向関数Ｈ［］に入力し、

Ｒ１＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ１とするとともに、

K'iso＝Ｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵K'isoとし、上記暗号鍵K'isoと受信した乱数Ａｎ２と上記データ送信装置に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ(Ｋｖ ‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｒ'２ ＝Ｈ［K'iso‖Ａｎ２‖Ｂｎ２］msb_p

その出力の最上位ｐビットを参照データＲ'２ とし、上記データ送信装置から送られてきたレスポンスデータＲ２と上記参照データＲ'２ とを比較して一致した場合に、上記レスポンスデータＲ１を上記データ送信装置に送り、

上記データ送信装置は、上記データ受信装置から送られてきたスポンスデータＲ１と上記参照データＲ'１ とを比較して一致した場合に、上記暗号鍵Ｋiso と上記データ受信装置に送った乱数Ａｎ２と受信した乱数Ｂｎ２を連結した連結データ（Ｋiso ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ（Ｋiso‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

Ｋasync＝Ｈ［Ｋiso ‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とし、

また、上記データ受信装置は、上記暗号鍵K'isoと受信した乱数Ａｎ２と上記データ送信装置に送った乱数Ｂｎ２を連結した連結データ（K'iso‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（K'iso‖Ａｎ２‖Ｂｎ２）を一方向関数Ｈ［］に入力し、

K'async＝Ｈ［K'iso‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵K'async とする

ことを特徴とする請求項１２記載のデータ伝送方法。

【請求項１５】　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、

上記インターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで送信し、上記データに関する関連データを第２の伝送モードで送信する送信制御手段と

を備えることを特徴とするデータ送信装置。

【請求項１６】　上記送信制御手段は、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで上記インターフェースを介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記インターフェースを介して送信する

ことを特徴とする請求項１５記載のデータ送信装置。

【請求項１７】　上記送信制御手段は、データ伝送に先立って、データ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する

ことを特徴とする請求項１５記載のデータ送信装置。

【請求項１８】　上記送信制御手段は、音楽データを上記第１の伝送モードで送信し、上記音楽データに関する関連データを第２の伝送モードで送信する

ことを特徴とする請求項１５記載のデータ送信装置。

【請求項１９】　上記インターフェースとしてＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを有し、

上記送信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous)伝送モードで送信し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで送信する

ことを特徴とする請求項１５記載のデータ送信装置。

【請求項２０】　上記送信制御手段は、データ伝送に先立って、データ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する

ことを特徴とする請求項１９記載のデータ送信装置。

【請求項２１】　伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、

上記インターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで受信し、上記データに関する関連データを第２の伝送モードで受信する受信制御手段と

を備えることを特徴とするデータ受信装置。

【請求項２２】　上記受信制御手段は、上記インターフェースを介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記インターフェースを介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する

ことを特徴とする請求項２１記載のデータ受信装置。

【請求項２３】　上記受信制御手段は、データ伝送に先立って、データ送信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する

ことを特徴とする請求項２１記載のデータ受信装置。

【請求項２４】　上記受信制御手段は、音楽データを上記第１の伝送モードで受信し、上記音楽データに関する関連データを第２の伝送モードで受信する

ことを特徴とする請求項２１記載のデータ受信装置。

【請求項２５】　上記インターフェースとしてＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを有し、

上記受信制御手段は、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous)伝送モードで受信し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで受信する

ことを特徴とする請求項２１記載のデータ受信装置。

【請求項２６】　上記受信制御手段は、データ伝送に先立って、データ送信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行する

ことを特徴とする請求項２５記載のデータ受信装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ送信装置からデータ受信装置にデータを一方向に伝送するデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置に関する。

【０００２】

【従来の技術】

近年、例えば家庭内において、複数のＡＶ機器をデジタルインターフェースを介して接続し、音楽情報や映像情報などのデジタルデータを伝送したり記録したりするようにしたシステムが普及しつつある。

【０００３】

例えば、デジタルバスであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス（以下、単にＩＥＥＥ１３９４シリアルバスという）のインターフェースを持つビデオカメラやＤＶＤプレーヤなどの機器では、データを高品質で記録することが可能であることから、著作権のあるデータが不正にコピーされてしまうのを防止する必要がある。

【０００４】

例えば、光磁気ディスク装置に映画情報を記録することが許可されているか否かを表すキーを記憶しておき、このキーを利用して、その光磁気ディスク装置が正当な装置すなわち著作権者からのライセンスを受けた装置であるか否かを認証するようにし、正当な装置として認証された光磁気ディスク装置のみに映画情報の記録を許可するようにすることが行われる。このような場合、映画情報を伝送する側の装置（以下、このような装置をソース(source)という）と、伝送を受けた装置（以下、このような装置をシンク(sink)という）との間で、相手側の装置が適正な装置であるか否かを認証する必要がある。

【０００５】

このようなシステムにおける著作権保護を目的として、様々な認証方式が提案

されている。これらの認証方式に用いられる認証プロトコルには、暗号アルゴリズムが用いられることが多い。

【０００６】

【発明が解決しようとする課題】

ところで、音楽データを機器間で伝送する際には、例えば、音楽データの伝送途中に伝送が止まったり、伝送できるデータ量が極端に減ったりすると、受信側で音楽の再生に必要なデータが得られなくなり、音楽が途切れてしまう虞があるので、ある程度の帯域を確保した状態で音楽データを伝送する必要がある。

【０００７】

一方、音楽データそのものではないが、音楽データに関連した情報として、例えば歌詞やアーティストの写真などを伝送する場合には、音楽データそのもの伝送する場合に比べて、リアルタイム性を必要としないので、伝送帯域が確保されていない伝送方式を用いて伝送することが可能である。一般に、伝送帯域が確保されていない伝送方式を用いる方が、伝送路全体の帯域を消費しないという点で望まれることが多い。

【０００８】

そこで、本発明の目的は、上述の如き従来の問題点に鑑み、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の２種類の伝送方式を採用して、データを確実に伝送することができるようにしたデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置を提供することにある。

【０００９】

また、本発明の他の目的は、伝送帯域の保証が必要なデータと上記データに関する関連データを異なる暗号鍵により暗号化して安全に伝送することができるようにしたデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置を提供することにある。

【００１０】

さらに、本発明の他の目的は、データ送信装置とデータ受信装置が互いの正当性を認証するとともに、暗号鍵を共有することができるようにしたデータ伝送システム、データ伝送方法、データ送信装置及びデータ受信装置を提供することに

ある。

【００１１】

【課題を解決するための手段】

本発明に係るデータ伝送システムは、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで送信し、上記データに関する関連データを第２の伝送モードで送信する送信制御手段とを備えるデータ送信装置と、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで受信し、上記データに関する関連データを第２の伝送モードで受信する受信制御手段とを備えるデータ受信装置とからなることを特徴とする。

【００１２】

本発明に係るデータ伝送方法は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介してデータ伝送を行うデータ伝送方法であって、伝送帯域の保証が必要なデータを第１の伝送モードで伝送し、上記データに関する関連データを第２の伝送モードで伝送することを特徴とする。

【００１３】

本発明に係るデータ送信装置は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで送信し、上記データに関する関連データを第２の伝送モードで送信する送信制御手段とを備えることを特徴とする。

【００１４】

本発明に係るデータ受信装置は、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースと、上記インターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで受信し、上記データに関する関連データを第２の伝送モードで受信する受信制御

手段とを備えることを特徴とする。

【００１５】

本発明では、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで伝送し、上記データに関する関連データを第２の伝送モードで伝送する。

【００１６】

上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで伝送し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで伝送することができる。また、データ伝送に先立って、データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行することができる。上記第１の伝送モードでは音楽データを伝送し、上記第２の伝送モードでは上記音楽データに関するデータを第２の伝送モードで伝送する。

【００１７】

データ送信装置とデータ受信装置との間のインターフェースとして、例えばＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４規格に準拠したインターフェースを採用することにより、伝送帯域の保証が必要なデータをアイソクロナス(Isochronous) 伝送モードで伝送し、上記データに関する関連データをアシンクロナス(Asynchronous)伝送モードで伝送することができる。また、データ伝送に先立って、上記データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルをアシンクロナス(Asynchronous)伝送モードで実行することができる。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照しながら説明する。

【００１９】

本発明は、各種デジタルＡＶ(Audio Visual)機器やパーソナルコンピュータ装置等の電子機器を、例えばＩＥＥＥ(Institute of Electrical Engineers) １３

９４バスを介して相互に接続することで、機器間でデータを送受信できるようにしたデータ伝送システム（ＡＶシステム）に適用される。このＡＶシステムは、デジタル衛星放送を受信して、受信データをダウンロード可能な構成が採られるものである。

【００２０】

このＡＶシステムを含むデジタル衛星放送システムの全体構成を図１に示してある。

【００２１】

この図１に示したデジタル衛星放送システムにおいて、デジタル衛星放送の地上局１０１には、テレビ番組素材サーバ１０６からのテレビ番組放送のための素材と、楽曲素材サーバ１０７からの楽曲データの素材と、音声付加情報サーバ１０８からの音声付加情報と、ＧＵＩ(Graphical User Interface)データサーバ１０９からのＧＵＩデータとが送られる。

【００２２】

テレビ番組素材サーバ１０６は、通常の放送番組の素材を提供するサーバである。このテレビ番組素材サーバから送られてくる音楽放送の素材は、動画及び音声とされる。例えば、音楽放送番組であれば、上記テレビ番組素材サーバ１０６の動画及び音声の素材を利用して、例えば新曲のプロモーション用の動画及び音声が放送されたりすることになる。

【００２３】

楽曲素材サーバ１０７は、オーディオチャンネルを使用して、オーディオ番組を提供するサーバである。このオーディオ番組の素材は音声のみとなる。この楽曲素材サーバ１０７は、複数のオーディオチャンネルのオーディオ番組の素材を地上局１０１に伝送する。

【００２４】

各オーディオチャンネルの番組放送ではそれぞれ同一の楽曲が所定の単位時間繰り返して放送される。各オーディオチャンネルは、それぞれ、独立しており、その利用方法としては各種考えられる。例えば、１つのオーディオチャンネルでは最新の日本のポップスの数曲を或る一定時間繰り返し放送し、他のオーディオ

チャンネルでは最新の外国のポップスの数曲を或る一定時間繰り返し放送するというようにされる。

【００２５】

音声付加情報サーバ１０８は、楽曲素材サーバ１０７から出力される楽曲の時間情報等を提供するサーバである。

【００２６】

ＧＵＩデータサーバ１０９は、ユーザが操作に用いるＧＵＩ画面を形成するための「ＧＵＩデータ」を提供する。例えば後述するような楽曲のダウンロードに関するＧＵＩ画面であれば、配信される楽曲のリストページや各楽曲の情報ページを形成するための画像データ、テキストデータ、アルバムジャケットの静止画を形成するためのデータなどを提供する。更には、ＡＶシステム１０３側にていわゆるＥＰＧ(Electrical Program Guide)といわれる番組表表示を行うのに利用されるＥＰＧデータもここから提供される。

【００２７】

なお、「ＧＵＩデータ」としては、例えばＭＨＥＧ(Multimedia Hypermedia Information Coding Experts Group)方式が採用される。ＭＨＥＧとは、マルチメディア情報、手順、操作などのそれぞれと、その組み合わせをオブジェクトとして捉え、それらのオブジェクトを符号化したうえで、タイトル（例えばＧＵＩ画面）として制作するためのシナリオ記述の国際標準とされる。また、このデジタル衛星放送システムではＭＨＥＧ－５を採用するものとする。

【００２８】

地上局１０１は上記テレビ番組素材サーバ１０６、楽曲素材サーバ１０７、音声付加情報サーバ１０８及びＧＵＩデータサーバ１０９から伝送された情報を多重化して送信する。

【００２９】

このデジタル衛星放送システムでは、テレビ番組素材サーバ１０６から伝送されたビデオデータはＭＰＥＧ(Moving Picture Experts Group)２方式により圧縮符号化され、オーディオデータはＭＰＥＧ２オーディオ方式により圧縮符号化される。また、楽曲素材サーバ１０７から伝送されたオーディオデータは、オーデ

ィオチャンネルごとに対応して、例えばＭＰＥＧ２オーディオ方式と、ＡＴＲＡＣ(Adoptive Tranform Acoustic Coding) 方式の何れか一方の方式により圧縮符号化される。

【００３０】

また、これらのデータは多重化の際、キー情報サーバ１１０からのキー情報を利用して暗号化される。

【００３１】

地上局１０１からの信号は衛星１０２を介して各家庭の受信設備（以降、ＡＶシステムともいう）１０３で受信される。衛星１０２には複数のトランスポンダが搭載されている。１つのトランスポンダは例えば３０Ｍｂｐｓの伝送能力を有している。各家庭のＡＶシステム１０３は、パラボラアンテナ１１１に接続されたＩＲＤ(Integrated Receiver Decorder)１１２と、このＩＲＤ１１２に接続されたモニタ装置１１４及びＭＤレコーダ／プレーヤ１とからなる。また、このＡＶシステム１０３は、ＩＲＤ１１２に対して操作を行うためのリモートコントローラ６４と、ＭＤレコーダ／プレーヤ１に対して操作を行うためのリモートコントローラ３２を備えている。

【００３２】

このＡＶシステム１０３では、パラボラアンテナ１１１で衛星１０２を介して放送されてきた信号が受信される。この受信信号がパラボラアンテナ１１１に取り付けられたＬＮＢ(Low Noize Block Down Converter)１１５で所定の周波数に変換され、ＩＲＤ１１２に供給される。

【００３３】

ＩＲＤ１１２における概略的な動作としては、受信信号から所定のチャンネルの信号を選局し、その選局された信号から番組としてのビデオデータ及びオーディオデータの復調を行ってビデオ信号、オーディオ信号として出力する。また、ＩＲＤ１１２では、番組としてのデータと共に多重化されて送信されてくる、ＧＵＩデータに基づいてＧＵＩ画面としての出力も行う。このようなＩＲＤ１１２の出力は、例えばモニタ装置１１４に対して供給される。これにより、モニタ装置１１４では、ＩＲＤ１１２により受信選局した番組の画像表示及び音声出力が

行われ、また、ユーザの操作に従ってＧＵＩ画面を表示させることが可能となる。

【００３４】

ＭＤレコーダ／プレーヤ１は、装填されたミニディスクに対するオーディオデータの記録／再生が可能な記録再生装置である。また、このＭＤレコーダ／プレーヤ１は、オーディオデータ（楽曲データ）及びこれに付随して関連付けされたアルバムジャケット等の静止画像データ（ピクチャファイル）、歌詞やライナーノーツ等のテキストデータ（テキストファイル）をディスクに記録し、かつ、記録されたこれらのピクチャファイル及びテキストファイル等のデータをオーディオデータの再生時間に同期させて再生出力することができるものである。

【００３５】

なお、上記オーディオデータに付随したピクチャファイル及びテキストファイル等のデータについては、後述するＭＤレコーダ／プレーヤ１での扱いに従って、便宜上「ＡＵＸデータ」ともいう。

【００３６】

ここで、このＡＶシステム１０３において、ＩＲＤ１１２及びＭＤレコーダ／プレーヤ１は、ＩＥＥＥ１３９４バス１１６によって相互接続されているものとされる。

【００３７】

つまり、ＡＶシステム１０３を構築しているＩＲＤ１１２及びＭＤレコーダ／プレーヤ１は、それぞれデータ伝送規格としてＩＥＥＥ１３９４に対応したデータインターフェイスを備えている。

【００３８】

これによって、このＡＶシステムでは、ＩＲＤ１１２にて受信された楽曲としてのオーディオデータ（ダウンロードデータ）を、ＡＴＲＡＣ方式により圧縮処理が施されたままの状態で直接取り込んで記録することができる。また、上記オーディオデータと共に送信側からアップロードされるＡＵＸデータをダウンロードして記録することも可能とされている。

【００３９】

ＩＲＤ１１２は、電話回線１０４を介して課金サーバ１０５と通信可能とされている。ＩＲＤ１１２には、各種情報が記憶されるＩＣカードが挿入されるようになっている。そして、例えば楽曲のオーディオデータのダウンロードが行われたとすると、これに関する履歴情報がＩＣカードに記憶される。このＩＣカードの情報は、電話回線１０４を介して所定の機会、タイミングで課金サーバ１０５に送られる。課金サーバ１０５は、この送られてきた履歴情報に従って金額を設定して課金を行い、ユーザに請求する。

【００４０】

これまでの説明から分かるように、本発明を適用したＡＶシステムを含むデジタル衛星放送システムでは、地上局１０１は、テレビ番組素材サーバ１０６からの音楽番組放送の素材となるビデオデータ及びオーディオデータと、楽曲素材サーバ１０７からのオーディオチャンネルの素材となるオーディオデータと、音声付加情報サーバ１０８からの音声データと、ＧＵＩデータサーバ１０９からのＧＵＩデータとを多重化して送信している。

【００４１】

そして、各家庭のＡＶシステム１０３でこの放送を受信すると、例えばモニタ装置１１４により、選局したチャンネルの番組を視聴することができる。また、番組のデータと共に送信されるＧＵＩデータを利用したＧＵＩ画面として、ＥＰＧ（Electrical Program Guide；電子番組ガイド）画面を表示させ、番組の検索等を行うことができる。また、例えば通常の番組放送以外の特定のサービス用のＧＵＩ画面を利用して所要の操作を行うことで、放送システムにおいて提供されている通常番組の視聴以外のサービスを享受することができる。

【００４２】

例えば、オーディオ（楽曲）データのダウンロードサービス用のＧＵＩ画面を表示させて、このＧＵＩ画面を利用して操作を行えば、ユーザが希望した楽曲のオーディオデータをダウンロードしてＭＤレコーダ／プレーヤ１によりディスクに記録して保存することが可能になる。

【００４３】

ここで、このデジタル衛星放送システムでは、地上局１０１から衛星１０２を介してのＡＶシステム１０３への送信を行うにあたり、ＤＳＭ－ＣＣ（デジタル蓄積メディア・コマンド・アンド・コントロール；Digital Strage Media-Command and Control)プロトコルを採用する。

【００４４】

ＤＳＭ－ＣＣ（ＭＰＥＧ－ｐａｒｔ６）方式は、既に知られているように、例えば、何らかのネットワークを介して、デジタル蓄積メディア（ＤＳＭ）に蓄積されたＭＰＥＧ符号化ビットストリームを取り出し(Retrieve)たり、或いはＤＳＭに対してストリームを蓄積(Store) するためのコマンドや制御方式を規定したものである。

【００４５】

そして、ＤＳＭ－ＣＣ方式によりデータ放送サービス（例えばＧＵＩ画面など）のコンテンツ（オブジェクトの集合）を伝送するためには、コンテンツの記述形式を定義しておく必要がある。このデジタル衛星放送システムでは、コンテンツの記述形式の定義として先に述べたＭＨＥＧが採用されている。

【００４６】

このデジタル衛星放送システムにおける地上局１０１は、図２のように構成されている。

【００４７】

図２に示した地上局１０１において、テレビ番組素材登録システム１３１は、テレビ番組素材サーバ１０６から得られた素材データをＡＶサーバ１３５に登録する。この素材データはテレビ番組送出システム１３９に送られ、ここでビデオデータは例えばＭＰＥＧ２方式で圧縮され、オーディオデータは、例えばＭＰＥＧ２オーディオ方式によりパケット化される。テレビ番組送出システム１３９の出力はマルチプレクサ１４５に送られる。

【００４８】

また、楽曲素材登録システム１３２では、楽曲素材サーバ１０７からの素材データ、つまりオーディオデータを、ＭＰＥＧ２オーディオエンコーダ１３６Ａ、

及びＡＴＲＡＣエンコーダ１３６Ｂに供給する。ＭＰＥＧ２オーディオエンコーダ１３６Ａ、ＡＴＲＡＣエンコーダ１３６Ｂでは、それぞれ供給されたオーディオデータについてエンコード処理（圧縮符号化）を行った後、ＭＰＥＧオーディオサーバ１４０Ａ及びＡＴＲＡＣオーディオサーバ１４０Ｂに登録させる。

【００４９】

ＭＰＥＧオーディオサーバ１４０Ａに登録されたＭＰＥＧオーディオデータは、ＭＰＥＧオーディオ送出システム１４３Ａに伝送されてここでパケット化された後、マルチプレクサ１４５に伝送される。ＡＴＲＡＣオーディオサーバ１４０Ｂに登録されたＡＴＲＡＣデータは、ＡＴＲＡＣオーディオ送出システム１４３Ｂに４倍速ＡＴＲＡＣデータとして送られ、ここでパケット化されてマルチプレクサ１４５に送出される。

【００５０】

また、音声付加情報登録システム１３３では、音声付加情報サーバ１０８からの素材データである音声付加情報を音声付加情報データベース１３７に登録する。この音声付加情報データベース１３７に登録された音声付加情報は、音声付加情報送出システム１４１に伝送され、同様にして、ここでパケット化されてマルチプレクサ１４５に伝送される。

【００５１】

また、ＧＵＩ用素材登録システム１３４では、ＧＵＩデータサーバ１０９からの素材データであるＧＵＩデータを、ＧＵＩ素材データベース１３８に登録する。

【００５２】

ＧＵＩ素材データベース１３８に登録されたＧＵＩ素材データは、ＧＵＩオーサリングシステム１４２に伝送され、ここで、ＧＵＩ画面としての出力が可能なデータ形式となるように処理が施される。

【００５３】

つまり、ＧＵＩオーサリングシステム１４２に伝送されてくるデータとしては、例えば、楽曲のダウンロードのためのＧＵＩ画面であれば、アルバムジャケットの静止画像データ、歌詞などのテキストデータ、更には、操作に応じて出力さ

れるべき音声データなどである。

【００５４】

上記した各データはいわゆるモノメディアといわれるが、ＧＵＩオーサリングシステム１４２では、ＭＨＥＧオーサリングツールを用いて、これらのモノメディアデータを符号化して、これをオブジェクトとして扱うようにする。

【００５５】

そして、ＧＵＩ画面の表示態様と操作に応じた画像音声の出力態様が得られるように上記オブジェクトの関係を規定したシナリオ記述ファイル（スクリプト）と共にＭＨＥＧ－５のコンテンツを作成する。

【００５６】

また、テレビ番組素材サーバ１０６の素材データを基とする画像・音声データ（ＭＰＥＧビデオデータ、ＭＰＥＧオーディオデータ）と、楽曲素材サーバ１０７の楽曲素材データを基とするＭＰＥＧオーディオデータ等も、ＧＵＩ画面に表示され、操作に応じた出力態様が与えられる。

【００５７】

従って、上記シナリオ記述ファイルとしては、上記ＧＵＩオーサリングシステム０４２では、上記したテレビ番組素材サーバ１０６の素材データを基とする画像・音声データ、楽曲素材サーバ１０７の楽曲素材データを基とするＭＰＥＧオーディオデータ、更には、音声付加情報サーバ１０８を基とする音声付加情報も必要に応じてオブジェクトとして扱われて、ＭＨＥＧのスクリプトによる規定が行われる。

【００５８】

なお、ＧＵＩオーサリングシステム１４２から伝送されるＭＨＥＧコンテンツのデータとしては、スクリプトファイル、及びオブジェクトとしての各種静止画データファイルやテキストデータファイルなどとなるが、静止画データは、例えばＪＰＥＧ(Joint Photograph Experts Group)方式で圧縮された６４０×４８０ピクセルのデータとされ、テキストデータは例えば８００文字以内のファイルとされる。

【００５９】

ＧＵＩオーサリングシステム１４２にて得られたＭＨＥＧコンテンツのデータはＤＳＭ－ＣＣエンコーダ１４４に伝送される。

【００６０】

ＤＳＭ－ＣＣエンコーダ１４４では、ＭＰＥＧ２フォーマットに従ったビデオ、オーディオデータのデータストリームに多重できる形式のトランスポートストリーム（以下ＴＳ(Transport Stream)とも略す）に変換して、パケット化されてマルチプレクサ１４５に出力される。

【００６１】

マルチプレクサ１４５においては、テレビ番組送出システム１３９からのビデオパケットおよびオーディオパケットと、ＭＰＥＧオーディオ送出システム１４３Ａからのオーディオパケットと、ＡＴＲＡＣオーディオ送出システム１４３Ｂからの４倍速オーディオパケットと、音声付加情報送出システム１４１からの音声付加情報パケットと、ＧＵＩオーサリングシステム１４２からのＧＵＩデータパケットとが時間軸多重化されると共に、キー情報サーバ１１０から出力されたキー情報に基づいて暗号化される。

【００６２】

マルチプレクサ１４５の出力は電波送出システム１４６に伝送され、ここで例えば誤り訂正符号の付加、変調、及び周波数変換などの処理を施された後、アンテナから衛星１０２に向けて送信される。

【００６３】

図３は、地上局１０１から衛星１０２に送信出力される際のデータの一例を示している。なお、この図３に示す各データは実際には時間軸多重化されているものである。また、各データは、図３に示すように、時刻ｔ１から時刻ｔ２の間が１つのイベントとされ、時刻ｔ２から次のイベントとされる。ここでいうイベントとは、例えば音楽番組のチャンネルであれば、複数楽曲のラインナップの組を変更する単位であり、時間的には３０分或いは１時間程度となる。

【００６４】

図３に示すように、時刻ｔ１から時刻ｔ２のイベントでは、通常の動画の番組

放送で、所定の内容Ａ１を有する番組が放送されている。また、時刻ｔ２から始めるイベントでは、内容Ａ２としての番組が放送されている。この通常の番組で放送されているのは動画と音声である。

【００６５】

ＭＰＥＧオーディオチャンネル（１）～（１０）は、例えば、チャンネルＣＨ１からＣＨ１０の１０チャンネル分用意される。このとき、各オーディオチャンネルＣＨ１，ＣＨ２，ＣＨ３・・・ＣＨ１０では、１つのイベントが放送されている間は同一楽曲が繰り返し送信される。つまり、時刻ｔ１～ｔ２のイベントの期間においては、オーディオチャンネルＣＨ１では楽曲Ｂ１が繰り返し送信され、オーディオチャンネルＣＨ２では楽曲Ｃ１が繰り返し送信され、以下同様に、オーディオチャンネルＣＨ１０では楽曲Ｋ１が繰り返し送信されることになる。これは、その下に示されている４倍速ＡＴＲＡＣオーディオチャンネル（１）～（１０）についても共通である。

【００６６】

つまり、図３において、ＭＰＥＧオーディオチャンネルと４倍速ＡＴＲＡＣオーディオチャンネルのチャンネル番号である（）内の数字が同じものは同じ楽曲となる。また、音声付加情報のチャンネル番号である（）内の数字は、同じチャンネル番号を有するオーディオデータに付加されている音声付加情報である。更に、ＧＵＩデータとして伝送される静止画データやテキストデータも各チャンネルごとに形成されるものである。これらのデータは、図４の（ａ）～（ｄ）に示すようにＭＰＥＧ２のトランスポートパケット内で時分割多重されて送信され、図４の（ｅ）～（ｈ）に示すようにしてＩＲＤ１１２内では各データパケットのヘッダ情報を用いて再構築される。

【００６７】

図５は、本発明に係るデータ伝送システムの構成を示すブロック図である。

【００６８】

このデータ伝送システムは、上述のデジタル衛星放送システムに含まれたＡＶシステム１０３を構成するものであって、上記ＩＲＤ１１２として機能するデータ送信装置１０と上記ＭＤレコーダ／プレーヤ１として機能するデータ受信装置

２０を備え、上記データ送信装置１０とデータ受信装置２０が伝送路３０を介して接続された構成となっている。

【００６９】

このデータ伝送システムにおいて、上記データ送信装置１０は、通信衛星から送られてくる衛星デジタル多チャネル放送番組を受信するセットトップボックスすなわち上述のＩＲＤ１１２であって、内部バス１１に接続された中央演算処理ユニット(CPU: Central Processing Unit)１２、メモリ１３、入力インターフェース１４、ユーザインターフェース１５、入出力インターフェース１６等により構成されている。上記入力インターフェース１４には衛星アンテナ１１５が接続されている。また、上記入出力インターフェース１６は、デジタルインターフェースであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス・インターフェース（以下、単にＩＥＥＥ１３９４インターフェースという）であって、ＩＥＥＥ１３９４バスからなる上記伝送路３０に接続されている。

【００７０】

このデータ送信装置１０において、上記ＣＰＵ１２は、上記メモリ１３に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース１５を介して入力される操作情報に応じて番組の選局動作等の各種制御動作を行うようになっている。

【００７１】

そして、このデータ送信装置１０は、上記受信アンテナ１１５が接続された上記入力インターフェース１４により衛星デジタル多チャネル放送信号の所望のチャンネルを選局して所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（テキストデータやＪＰＥＧデータ等の関連データ）を受信し、受信した音楽データ及びメタデータ（関連データ）を上記入出力インターフェース１６から上記伝送路３０に送信する。

【００７２】

また、上記データ受信装置２０は、上記データ送信装置１０すなわちセットトップボックスにより受信したコンテンツ（音楽データ）及びメタデータ（関連デ

ータ）を磁気テープや光磁気ディスクなどの記録媒体を介して記録／再生する記録／再生装置であって、内部バス２１に接続された中央演算処理ユニット(CPU: Central Processing Unit)２２、メモリ２３、入出力インターフェース２４、ユーザインターフェース２５、メディアアクセス部２６等により構成されている。上記入出力インターフェース２４は、デジタルインターフェースであるＩＥＥＥ(The International of Electrical and Electronics Engineers,Inc.)１３９４ハイ・パフォーマンス・シリアル・バス・インターフェース（以下、単にＩＥＥＥ１３９４インターフェースという）であって、ＩＥＥＥ１３９４バスからなる上記伝送路３０が接続されている。

【００７３】

図６は、上記伝送路３０として実際に用いられるＩＥＥＥ１３９４バスケーブルの構造例を示している。

【００７４】

この図６においては、コネクタ６００Ａと６００Ｂがケーブル６０１を介して接続されていると共に、ここでは、コネクタ６００Ａと６００Ｂのピン端子として、ピン番号１～６の６ピンが使用される場合を示している。

【００７５】

コネクタ６００Ａ，６００Ｂに設けられる各ピン端子については、ピン番号１は電源（ＶＰ）、ピン番号２はグランド（ＶＧ）、ピン番号３はＴＰＢ１、ピン番号４はＴＰＢ２、ピン番号５はＴＰＡ１、ピン番号５はＴＰＡ２とされている。

【００７６】

そして、コネクタ６００Ａ－６００Ｂ間の各ピンの接続形態は、

ピン番号１（ＶＰ）－ピン番号１（ＶＰ）

ピン番号２（ＶＧ）－ピン番号２（ＶＧ）

ピン番号３（ＴＰＢ１）－ピン番号５（ＴＰＡ１）

ピン番号４（ＴＰＢ２）－ピン番号６（ＴＰＡ２）

ピン番号５（ＴＰＡ１）－ピン番号３（ＴＰＢ１）

ピン番号６（ＴＰＡ２）－ピン番号３（ＴＰＢ２）

のようになっている。そして、上記ピン接続の組のうち、

ピン番号３（ＴＰＢ１）－ピン番号５（ＴＰＡ１）

ピン番号４（ＴＰＢ２）－ピン番号６（ＴＰＡ２）

の２本のツイスト線の組により、差動で信号を相互伝送する信号線６０１Ａを形成し、

ピン番号５（ＴＰＡ１）－ピン番号３（ＴＰＢ１）

ピン番号６（ＴＰＡ２）－ピン番号３（ＴＰＢ２）

の２本のツイスト線の組により、差動で信号を相互伝送する信号線６０１Ｂを形成している。

【００７７】

上記２組の信号線６０１Ａ及び信号線６０１Ｂにより伝送される信号は、図７の（ａ）に示すデータ信号(Data)と、図７の（ｂ）に示すストローブ信号(Strobe)である。

【００７８】

図７の（ａ）に示すデータ信号は、信号線６０１Ａ又は信号線６０１Ｂの一方を使用してＴＰＢ１，２から出力され、ＴＰＡ１，２に入力される。

【００７９】

また、図７の（ｂ）に示すストローブ信号は、データ信号と、このデータ信号に同期する伝送クロックとについて所定の論理演算を行うことによって得られる信号であり、実際の伝送クロックよりは低い周波数を有する。このストローブ信号は、信号線６０１Ａ又は信号線６０１Ｂのうち、データ信号伝送に使用していない他方の信号線を使用して、ＴＰＡ１，２から出力され、ＴＰＢ１，２に入力される。

【００８０】

例えば、図７の（ａ），（ｂ）に示すデータ信号及びストローブ信号が、或るＩＥＥＥ１３９４対応の機器に対して入力されたとすると、この機器においては、入力されたデータ信号とストローブ信号とについて所定の論理演算を行って、図７の（ｃ）に示すような伝送クロック(Clock) を生成し、所要の入力データ信号処理に利用する。

【００８１】

ＩＥＥＥ１３９４規格では、このようなハードウェア的データ伝送形態を採ることで、高速な周期の伝送クロックをケーブルによって機器間で伝送する必要をなくし、信号伝送の信頼性を高めるようにしている。

【００８２】

なお、上記説明では６ピンの仕様について説明したが、ＩＥＥＥ１３９４フォーマットでは電源（ＶＰ）とグランド（ＶＧ）を省略して、２組のツイスト線である信号線６０１Ａ及び信号線６０１Ｂのみからなる４ピンの仕様も存在する。例えば、このＡＶシステム１０３におけるＭＤレコーダ／プレーヤ１では、実際には、この４ピン仕様のケーブルを用いることで、ユーザにとってより簡易なシステムを提供できるように配慮している。

【００８３】

ここで、ＩＥＥＥ１３９４規格では、ＩＥＥＥ１３９４バスを介して接続されたネットワーク内で行われる伝送動作をサブアクションと呼び、次の２種類のサブアクションが規定されている。すなわち、２つのサブアクションとして、「アシンクロナス(Asynchronous)」と呼ばれる非同期伝送モード、及び、「アイソクロナス(Isochronous)」と呼ばれる伝送帯域を保証した同期伝送モードが定義されている。

【００８４】

すなわち、ＩＥＥＥ１３９４規格では、図８に示すようにIsochronous cycle(nominal cycle)の周期を繰り返すことによって送信を行う。この場合、１Isochronous cycleは、１２５μｓｅｃとされ、帯域としては１００ＭＨｚに相当する。なお、Isochronous cycle の周期としては１２５μｓｅｃ以外とされても良いことが規定されている。そして、このIsochronous cycle ごとに、データをパケット化して送信する。

【００８５】

このIsochronous cycleの先頭には、１Isochronous cycleの開始を示すCycle Start Packetが配置される。

【００８６】

このCycle Start Packetは、Cycle Masterとして定義されたＩＥＥＥ１３９４ネットワークシステム内の特定の１機器によってその発生タイミングが指示される。

【００８７】

Cycle Start Packetに続いては、Isochronous Packetが優先的に配置される。Isochronous Packetは、図８のように、チャンネルごとにパケット化されたうえで時分割的に配列されて転送される(Isochronous subactions)。また、Isochronous subactions内においてパケット毎の区切りには、Isochronous gap といわれる休止区間（例えば０．０５μｓｅｃ）が設けられる。

【００８８】

このように、ＩＥＥＥ１３９４システムでは、１つの伝送線路によってIsochronous データをマルチチャンネルで送受信することが可能とされている。

【００８９】

ここで、例えばこのＡＶシステムにおけるＭＤレコーダ／プレーヤ１が対応するＡＴＲＡＣデータ（圧縮オーディオディオデータ）をIsochronous 方式により送信することを考えた場合、ＡＴＲＡＣデータが１倍速の転送レート１．４Ｍｂｐｓであるとすれば、１２５μｓｅｃである１Isochronous cycle 周期ごとに、少なくともほぼ２０数MバイトのＡＴＲＡＣデータをIsochronous Packetとして伝送すれば、時系列的な連続性（リアルタイム性）が確保されることになる。

【００９０】

例えば、或る機器がＡＴＲＡＣデータを送信する際には、ＩＥＥＥ１３９４ネットワークシステム内のＩＲＭ(Isochronous Resource Manager)に対して、ＡＴＲＡＣデータのリアルタイム送信が確保できるだけの、Isochronous パケットのサイズを要求する。ＩＲＭでは、現在のデータ伝送状況を監視して許可／不許可を与え、許可が与えられれば、指定されたチャンネルによって、ＡＴＲＡＣデータをIsochronous Packetにパケット化して送信することが出来る。これがＩＥＥＥ１３９４インターフェイスにおける帯域予約といわれるものである。

【００９１】

Isochronous cycle の帯域内においてIsochronous subactionsが使用していない残りの帯域を用いて、Asynchronous subactions、即ちAsynchronous のパケット送信が行われる。

【００９２】

図８では、Packet A, Packet B の２つのAsynchronous Packetが送信されている例が示されている。Asynchronous Packet の後には、ack gap(０．０５μｓｅｃ)の休止期間を挟んで、ＡＣＫ（Acknowledge）といわれる信号が付随する。ＡＣＫは、Asynchronous Transactionの過程において、何らかのAsynchronousデータの受信が有ったことを送信側(Controller)に知らせるためにハードウェア的に受信側(Target)から出力される信号である。

【００９３】

また、Asynchronous Packet 及びこれに続くＡＣＫからなるデータ伝送単位の前後には、１０μｓｅｃ程度のsubaction gap といわれる休止期間が設けられる。

【００９４】

ここで、Isochronous PacketによりＡＴＲＡＣデータを送信し、上記ＡＴＲＡＣデータに付随するＡＵＸデータファイルをAsynchronous Packet により送信するようにすれば、見かけ上、ＡＴＲＡＣデータとＡＵＸデータファイルとを同時に送信することが可能となる。

【００９５】

ここで、Asynchronous伝送は１対１のユニキャスト伝送であり、ブロードキャスト伝送を行うIsochronous 伝送に比べて盗聴が難しいという性質がある。

【００９６】

このデータ伝送システムでは、伝送帯域を確保できるIsochronous 伝送を用いて音楽データを伝送し、関連情報は、Asynchronous 伝送を用いて伝送する。

【００９７】

そして、データ受信装置２０は、入出力インターフェース２４を介して音楽データと関連情報を受信し、それが記録可能であれば、メディアアクセス部２６に

より上記磁気テープや光磁気ディスクなどの記録媒体に記録する。

【００９８】

上記記録媒体に記録された音楽データと関連情報はメディアアクセス部２６により再生され、音楽データは、アナログ信号に変換されアナログ音声出力端子２６Ａから出力され、関連データは映像出力端子２６Ｂから出力される。また、上記メディアアクセス部２６により再生され音楽データと関連情報は、ＩＥＥＥ１３９４インターフェースを介してさらに他の機器に伝送されることがある。

【００９９】

また、データ受信装置２０は、記録禁止の音楽データを受信した場合には、上記メディアアクセス部２６により記録媒体に記録することなく、単に音楽データをアナログ信号に変換してアナログ音声出力端子２６Ａから出力する。

【０１００】

このデータ受信装置２０において、上記ＣＰＵ２２は、上記メモリ２３に記憶されている制御プログラムにしたがって動作して、上記ユーザインターフェース２５を介して入力される操作情報に応じて、上記メディアアクセス部２６による記録動作等の各種制御動作を行うようになっている。

【０１０１】

そして、このデータ伝送システムでは、受信アンテナ１１５を介してデータ送信装置１０により受信した所望のチャンネルのコンテンツ（音楽データ）及びメタデータ（関連データすなわちテキストデータやＪＰＥＧデータ等）を、それぞれ別の暗号方式、暗号鍵を用いて暗号化してデータ受信装置２０に伝送する。

【０１０２】

すなわち、データ送信装置１０の要部構成を図９に示してあるように、上記データ送信装置１０の入力インターフェース１４は、衛星デジタル多チャネル放送信号の所望のチャンネルを選局するデマルチプレクサ(DEMUX) １４Ａと、このデマルチプレクサ(DEMUX) １４Ａにより選局された所望のチャンネルのトランスポートストリームを復号するデコーダ(DEC) １４Ｂを備え、また、入出力インターフェース１６は、上記デコーダ(DEC) １４Ｂにより復号された所望のチャンネルのトランスポートストリームに含まれているコンテンツ（音楽データ）及びメタ

データ（関連データすなわちテキストデータやＪＰＥＧデータ等）を分離するデータ分離回路１６Ａと、このデータ分離回路１６Ａにより分離されたコンテンツ（音楽データ）を暗号鍵Ｋiso により第１の暗号方式で暗号化してIsochronous Packetを生成する第１のエンコーダ１６Ｂと、上記データ分離回路１６Ａにより分離されたメタデータ（関連データ）を暗号鍵Ｋasync により第２の暗号方式で暗号化してAsynchronous Packetを生成する第１のエンコーダ１６Ｃを備える。

【０１０３】

そして、上記データ送信装置１０における入出力インターフェース１６は、ＣＰＵ１２により制御されて、図１０のフローチャートに示すように動作する。すなわち、上記入出力インターフェース１６は、上記入力インターフェース１４を介して受信された所望のチャンネルのトランスポートストリームが入力されると（ステップＳ１）、入力されたトランスポートストリームに含まれているデータがコンテンツ（音楽データ）であるかメタデータ（関連データ）であるかを判定し（ステップＳ２）、コンテンツ（音楽データ）である場合には、そのコンテンツ（音楽データ）を暗号鍵Ｋiso により第１の暗号方式で暗号化し（ステップＳ３）、第１の暗号方式で暗号化したコンテンツ（音楽データ）をIsochronous Packetとして伝送する処理を行う（ステップＳ４）。また、入力されたトランスポートストリームに含まれているデータがメタデータ（関連データ）である場合には、そのメタデータ（関連データ）を暗号鍵ＫAsync により第２の暗号方式で暗号化し（ステップＳ５）、第２の暗号方式で暗号化したメタデータ（関連データ）をAsynchronous Packet として伝送する処理を行う（ステップＳ６）。

【０１０４】

このデータ伝送システムでは、上記データ伝送に先立って、データ送信装置１０とデータ受信装置２０の間で相互認証と２種類の暗号鍵の共有プロトコルを実行する。具体的には、図１１のフローチャートに示すような認証・鍵共有プロトコルを実行してから、データ伝送を行う。なお、このデータ伝送システムにおけるデータ送信装置１０側の処理手順を図１２のフローチャートに示すとともに、データ受信装置２０側の処理手順を図１３のフローチャートに示す。

【０１０５】

上記認証・鍵共有プロトコルを示す図１１では、データ送信装置１０をSource DeviceAで表し、データ受信装置２０をSink DeviceBで表す。これらの機器は、自分が正当であることを示す情報Ｋｖが機器の製造時に与えられ、秘密に保持している。

【０１０６】

そして、このデータ伝送システムおいて、上記データ送信装置１０すなわちセットトップボックスのＣＰＵ１２は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース１６から上記伝送路３０を介してデータ受信装置２０に送信する（ステップＳ１０）。

【０１０７】

上記データ受信装置２０すなわち記録装置のＣＰＵ２２は、上記入出力インターフェース２４に接続された上記伝送路３０を介して上記データ送信装置１０から送られてくるスタートコマンド(START command) を受信したら（ステップＳ２０）、認証・鍵共有プロトコルの開始要求(Request authentication)とｍ（例えばｍ＝６４）ビットの２つの乱数Ｂｎ１，Ｂｎ２を生成して上記データ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ２１）。

【０１０８】

上記データ送信装置１０のＣＰＵ１２は、上記入出力インターフェース１４に接続された上記伝送路３０を介して上記データ受信装置２０から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数Ｂｎ１，Ｂｎ２を受信したら（ステップＳ１１）、ｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置１０に入出力インターフェース１４を介して送る（ステップＳ１２）。

【０１０９】

上記データ受信装置１０は、上記データ送信装置１０から送られてくる２つの乱数Ａｎ１，Ａｎ２を受信する（ステップＳ２２）。

【０１１０】

そして、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示

す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１で受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ２＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットをレスポンスデータＲ２とし、このレスポンスデータＲ２を上記データ受信装置２０に入出力インターフェース１４を介して送る（ステップＳ１３）。ここで、Ｘ‖Ｙは、ＸとＹとのビット連結を示す。

【０１１１】

上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０から送られてくるレスポンスデータＲ２を受信し（ステップＳ２３）、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ１と上記ステップＳ２１でデータ送信装置１０に送った乱数Ａｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ１＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

その出力の最上位ｍビットをレスポンスデータＲ１とし、このレスポンスデータＲ１を上記データ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ２４）。

【０１１２】

上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０から送られてくるレスポンスデータＲ１を受信する（ステップＳ１４）。

【０１１３】

さらに、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１で受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ’１＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_m

その出力の最上位ｍビットを参照データＲ’１ とする（ステップＳ１５）。

【０１１４】

そして、上記データ送信装置１０のＣＰＵ１２は、上記参照データＲ’１ を上記ステップＳ１４で受信したレスポンスデータＲ１と比較する（ステップＳ１６）。このステップＳ１６において、レスポンスデータＲ１が参照データＲ’１ と一致しなければ、上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【０１１５】

上記ステップＳ１６においてレスポンスデータＲ１が参照データＲ’１ と一致した場合には、上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０を正当な機器であると判断し、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１で受信した乱数Ｂｎ１を連結した連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋiso ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送るデータを暗号化するために使用する暗号鍵Ｋiso とする。また、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１で受信した乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋasync＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とする（ステップＳ１７）。

【０１１６】

また、上記データ受信装置２０のＣＰＵ２２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ２と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２)を生成し、この連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

R'２＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］msb_m

その出力の最上位ｍビットを参照データR'２ とする（ステップＳ２５）。

【０１１７】

そして、上記データ受信装置２０のＣＰＵ２２は、この参照データR'２ を上記ステップＳ２３で受信したレスポンスデータＲ２と比較する（ステップＳ２６）。このステップＳ２６において、レスポンスデータＲ２が参照データR'２ と一致しなければ、上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【０１１８】

また、上記ステップＳ２６においてレスポンスデータＲ２が参照データR'２と一致した場合には、上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０を正当な機器であると判断し、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ１と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ１を連結した連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

K'iso ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_m

その出力の最下位ｍビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵K'iso とする。また、自分が正当であることを示す情報Ｋｖと上記ステップＳ２２で受信した乱数Ａｎ２と上記ステップＳ２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ(Ｋｖ‖Ａｎ２‖Ｂｎ２)をハッシュ関数Ｈａｓｈ［］に入力し、

K'async＝Ｈａｓｈ［Ｋｖ‖Ａｎ２‖Ｂｎ２］lsb_m

その出力の最下位ｍビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵K'async とする（ステップＳ２７）。

【０１１９】

このデータ伝送システムでは、データ伝送に先立って、上記認証・鍵共有プロトコルをデータ送信装置１０とデータ受信装置２０の間でＩＥＥＥ１３９４のAsynchronous伝送によって実行することにより、データ送信装置１０とデータ受信装置２０が、相互に正当性を認証するとともに、Isochronous 伝送で暗号化した

データを送るための暗号鍵とAsynchronous伝送で暗号化したデータを送るための暗号鍵を共有することができる。

【０１２０】

そして、このデータ伝送システムでは、上記認証・鍵共有プロトコルを実行した後に、データ送信装置１０から音楽データを暗号鍵Ｋiso で暗号化してIsochronous 伝送で送信し、また、関連データを暗号鍵Ｋasync で暗号化してAsynchronous伝送で送信し（ステップＳ１８）、データ受信装置２０は、Isochronous 伝送により送られてくる音楽データを暗号鍵K'isoで復号し、また、Asynchronous 伝送で送られてくる関連データを暗号鍵K'asyncで復号する（ステップＳ２８）。

【０１２１】

すなわち、上記認証・鍵共有プロトコルの実行後は、データ受信装置２０は、データ送信装置１０からIsochronous 伝送により送られてくる音楽データを暗号鍵K'isoで復号し、また、Asynchronous伝送で送られてくる関連データを暗号鍵K'asyncで復号して、それぞれの平文データを得ることができる。

【０１２２】

ここで、このデータ伝送システムおいて、上記データ伝送に先立って実行する認証・鍵共有プロトコルの他の例を図１４のフローチャートに示す。この場合のデータ送信装置１０側の処理手順を図１５のフローチャートに示すとともに、データ受信装置２０側の処理手順を図１６のフローチャートに示す。

【０１２３】

上記認証・鍵共有プロトコルを示す図１４では、データ送信装置１０をSource DeviceＡで表し、データ受信装置２０をSink DeviceＢで表す。これらの機器は、自分が正当であることを示す情報Ｋｖが機器の製造時に与えられ、秘密に保持している。

【０１２４】

そして、このデータ伝送システムおいて、上記データ送信装置１０すなわちセットトップボックスのＣＰＵ１２は、先ず、データの伝送を開始するためのスタートコマンドを上記入出力インターフェース１６から上記伝送路３０を介してデ

ータ受信装置２０に送信する（ステップＳ１１０）。

【０１２５】

上記データ受信装置２０すなわち記録装置のＣＰＵ２２は、上記入出力インターフェース２４に接続された上記伝送路３０を介して上記データ送信装置１０から送られてくるスタートコマンド(START command) を受信したら（ステップＳ１２０）、認証・鍵共有プロトコルの開始要求(Request authentication)とｍ（例えばｍ＝６４）ビットの２つの乱数Ｂｎ１，Ｂｎ２を生成して上記データ送信装置１０に入出力インターフェース２４を介して送る（ステップＳ１２１）。

【０１２６】

上記データ送信装置１０のＣＰＵ１２は、上記入出力インターフェース１４に接続された上記伝送路３０を介して上記データ受信装置２０から送られてくる認証・鍵共有プロトコルの開始要求(Request authentication)と乱数Ｂｎ１，Ｂｎ２を受信したら（ステップＳ１１１）、ｍビットの２つの乱数Ａｎ１，Ａｎ２を生成して上記データ受信装置１０に入出力インターフェース１４を介して送る（ステップＳ１１２）。

【０１２７】

上記データ受信装置１０は、上記データ送信装置１０から送られてくる２つの乱数Ａｎ１，Ａｎ２を受信する（ステップＳ１２２）。

【０１２８】

そして、上記データ送信装置１０のＣＰＵ１２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１１で受信した乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ’１ ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビット（例えばｐ＝６４）を参照データＲ’１ とするとともに、

Ｋiso ＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎ（例えばｎ＝６４）ビットをIsochronous 伝送で送るデータを暗号化す

るために使用する暗号鍵Ｋiso とする（ステップＳ１１３）。ここで、Ｘ‖Ｙは、ＸとＹとのビット連結を示す。

【０１２９】

そして、上記データ送信装置１０のＣＰＵ１２は、このようにして算出した暗号鍵Ｋiso と上記ステップＳ１１２でデータ受信装置２０に送った乱数Ａｎ１と上記ステップＳ１１１で受信した乱数Ｂｎ１を連結した連結データ（Ｋiso ‖Ａｎ１‖Ｂｎ１)を生成し、この連結データ(Ｋiso ‖Ａｎ１‖Ｂｎ１）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ２＝Ｈａｓｈ［Ｋiso‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ２とする（ステップＳ１１４）

また、上記データ受信装置２０のＣＰＵ２２は、自分が正当であることを示す情報Ｋｖと上記ステップＳ１２２で受信した乱数Ａｎ１と上記ステップＳ１２１でデータ送信装置１０に送った乱数Ｂｎ１を連結した連結データ（Ｋｖ‖Ａｎ１‖Ｂｎ１）を生成し、この連結データ(Ｋｖ‖Ａｎ１‖Ｂｎ１)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ１　＝Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］msb_p

その出力の最上位ｐビットをレスポンスデータＲ１とし、

K'iso=Ｈａｓｈ［Ｋｖ‖Ａｎ１‖Ｂｎ１］lsb_n

最下位ｎビットをIsochronous 伝送で送られてくるデータを復号するために使用する暗号鍵K'isoとする（ステップＳ１２３）。

【０１３０】

また、上記データ受信装置２０のＣＰＵ２２は、このようにして算出した暗号鍵K'isoと上記ステップＳ１２２で受信した乱数Ａｎ２と上記ステップＳ１２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ（Ｋｖ‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ(Ｋｖ ‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

Ｒ'２ ＝Ｈａｓｈ［K'iso‖Ａｎ２‖Ｂｎ２］msb_p

その出力の最上位ｐビットを参照データＲ'２ とする（ステップＳ１２４）。

【０１３１】

そして、上記データ送信装置１０のＣＰＵ１２は、ステップＳ１１４で算出したレスポンスデータＲ２を上記データ受信装置２０に入出力インターフェース１４を介して送る（ステップＳ１１５）。

【０１３２】

上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０から送られてくるレスポンスデータＲ２を受信し（ステップＳ１２５）、上記ステップＳ１２４で算出した参照Ｒ’２ と比較する（ステップＳ１２６）。このステップＳ１２６において、レスポンスデータＲ１が参照データＲ’１ と一致しなければ、上記データ受信装置２０のＣＰＵ２２は、上記データ送信装置１０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【０１３３】

上記ステップＳ１２６においてレスポンスデータＲ２が参照データＲ’２ と一致した場合には、上記データ受信装置２０のＣＰＵ２２は、上記ステップＳ１２３で算出したレスポンスデータＲ１を上記データ送信装置１０に入出力インターフェース１４を介して送る（ステップＳ１２７）。

【０１３４】

上記データ送信装置１０のＣＰＵ１０は、上記データ受信装置２０から送られてくるレスポンスデータＲ１を受信し（ステップＳ１１６）、上記ステップＳ１１３で算出した参照データＲ’１ と比較する（ステップＳ１１７）。このステップＳ１１７において、レスポンスデータＲ１が参照データＲ’１ と一致しなければ、上記データ送信装置２０のＣＰＵ１２は、上記データ受信装置２０が不正な機器であると判断して、この認証・鍵共有プロトコルを終了する。

【０１３５】

上記ステップＳ１１７においてレスポンスデータＲ１が参照データＲ’１ と一致した場合には、上記データ送信装置１０のＣＰＵ１２は、上記データ受信装置２０を正当な機器であると判断し、上記ステップＳ１１３で算出した暗号鍵Ｋｉｓｏと上記ステップＳ１１２でデータ受信装置２０に送った乱数Ａｎ２と上記ステップＳ１１１で受信した乱数Ｂｎ２を連結した連結データ（Ｋｉｓｏ ‖ Ａｎ２ ‖ Ｂ

ｎ２)を生成し、この連結データ（Ｋiso ‖Ａｎ２‖Ｂｎ２)をハッシュ関数Ｈａｓｈ［］に入力し、

Ｋasync＝Ｈａｓｈ［Ｋiso ‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビット（例えばｑ＝６４）をAsynchronous伝送で送るデータを暗号化するために使用する暗号鍵Ｋasync とする（ステップＳ１１８）。

【０１３６】

また、上記データ受信装置２０のＣＰＵ２２は、上記ステップＳ１２３で算出した暗号鍵K'isoと上記ステップＳ１２２で受信した乱数Ａｎ２と上記ステップＳ１２１でデータ送信装置１０に送った乱数Ｂｎ２を連結した連結データ（K'iso‖Ａｎ２‖Ｂｎ２）を生成し、この連結データ（K'iso‖Ａｎ２‖Ｂｎ２）をハッシュ関数Ｈａｓｈ［］に入力し、

K'async＝Ｈａｓｈ［K'iso‖Ａｎ２‖Ｂｎ２］lsb_q

その出力の最下位ｑビットをAsynchronous伝送で送られてくるデータを復号するために使用する暗号鍵K'async とする（ステップＳ１２８）。

【０１３７】

このデータ伝送システムでは、データ伝送に先立って、上記認証・鍵共有プロトコルをデータ送信装置１０とデータ受信装置２０の間でＩＥＥＥ１３９４のAsynchronous伝送によって実行することにより、データ送信装置１０とデータ受信装置２０が、相互に正当性を認証するとともに、Isochronous 伝送で暗号化したデータを送るための暗号鍵とAsynchronous伝送で暗号化したデータを送るための暗号鍵を共有することができる。

【０１３８】

すなわち、上記認証・鍵共有プロトコルの実行後は、データ送信装置１０から音楽データを暗号鍵Ｋiso で暗号化してIsochronous 伝送で送信し、また、関連データを暗号鍵Ｋasync で暗号化してAsynchronous伝送で送信することによって（ステップＳ１１９）、データ受信装置２０は、Isochronous 伝送により送られてくる音楽データを暗号鍵K'isoで復号し、また、Asynchronous伝送で送られてくる関連データを暗号鍵K'asyncで復号することにより（ステップＳ１２９）、それぞれの平文データを得ることができる。

【０１３９】

ここで、一般にIsochronous 伝送とAsynchronous伝送では性質が違うので、それぞれに用いられる暗号アルゴリズムやモードもそれぞれに適したものが使用される。そこで、Asynchronous伝送に使用される暗号アルゴリズムがIsochronous伝送に使用されるものに比べて強度的に弱い場合、Asynchronous伝送に使用される暗号鍵Ｋasyncは、Isochronous 伝送に使用される暗号鍵Ｋisoに比べて比較的容易に露呈してしまうことになる。図１１に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報Ｋｖから暗号鍵Ｋasyncと暗号鍵Ｋisoを直接生成しているので、暗号鍵Ｋasyncが露呈してしまうと、例えば総当たり攻撃により情報Ｋｖが露呈してしまうことになる。

【０１４０】

これに対して、図１４に示した認証・鍵共有プロトコルでは、各機器が秘密に保持している自分が正当であることを示す情報Ｋｖから暗号鍵Ｋiso を生成し、この暗号鍵Ｋiso から暗号鍵Ｋasyncを生成しているので、暗号鍵Ｋasyncが露呈しても、攻撃者は、一方向性関数Ｈａｓｈを一度攻撃するだけでは情報Ｋｖを得ることはできず、総当たり攻撃により暗号鍵Ｋiso を求めて、しかる後に情報Ｋｖを総当たり攻撃しなければならない。

【０１４１】

すなわち、図１４に示した認証・鍵共有プロトコルでは、図１１に示した認証・鍵共有プロトコルと比較して、各機器が秘密に保持している自分が正当であることを示す情報Ｋｖが露呈しにくく、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

【０１４２】

なお、上述のデータ伝送システムでは、各認証・鍵共有プロトコルを実行することによりデータ送信装置１０とデータ受信装置２０の間で共有される暗号鍵Ｋiso, Ｋ'iso 及び暗号鍵Ｋasync, Ｋ'async を用いて伝送データを暗号化／復号するようにしているが、実際に伝送するデータを暗号化／復号するための暗号鍵（コンテンツキー）は別に用意して、暗号鍵Ｋiso, Ｋ'iso 及び暗号鍵Ｋasync, Ｋ'asyncを用いてコンテンツキーをデータ送信装置１０とデータ受信装置２０

の間で共有することもできる。

【０１４３】

【発明の効果】

以上のように本発明では、伝送帯域が保証された第１の伝送モードと伝送帯域が保証されていない第２の伝送モードを持つインターフェースを介して、伝送帯域の保証が必要なデータを第１の伝送モードで伝送し、上記データに関する関連データを第２の伝送モードで伝送するので、伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の２種類の伝送方式を採用して、データを確実に伝送することができる。

【０１４４】

また、本発明では、上記伝送帯域の保証が必要なデータを第１の暗号鍵で暗号化して第１の伝送モードで伝送し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで伝送するにより、伝送帯域の保証が必要なデータと上記データに関する関連データを安全に伝送することができる。

【０１４５】

さらに、本発明では、データ伝送に先立って、データ送信装置とデータ受信装置と間で相互認証及び複数の暗号鍵を共有するためのプロトコルを実行することによって、データ送信装置とデータ受信装置が互いの正当性を認証するとともに、暗号鍵を共有することができ、伝送帯域の保証が必要なデータと上記データに関する関連データを安全にかつ確実に伝送することができる。

【図面の簡単な説明】

【図１】

本発明を適用したＡＶシステムを含むデジタル衛星放送システムの全体構成をブロック図である。

【図２】

上記デジタル衛星放送システムにおける地上局の構成をブロック図である。

【図３】

上記地上局から送信されるデータを示す図である。

【図４】

送信データの時分割多重化構造を示す説明図である。

【図５】

本発明を適用したデータ伝送システムの構成を示すブロック図である。

【図６】

ＩＥＥＥ１３９４バスケーブルの構造を模式的に示す説明図である。

【図７】

ＩＥＥＥ１３９４における信号伝送形態を示す説明図である。

【図８】

ＩＥＥＥ１３９４におけるＰａｃｋｅｔ送信の概要を示す説明図である。

【図９】

上記データ伝送システムにおけるデータ送信装置の要部構成を示すブロック図である。

【図１０】

上記データ送信装置の動作を示すフローチャートである。

【図１１】

上記データ伝送システムにおけるデータ伝送の手順を示すフローチャートである。

【図１２】

上記データ伝送システムにおけるデータ送信装置側の処理手順を示すフローチャートである。

【図１３】

上記データ伝送システムにおけるデータ受信装置側の処理手順を示すフローチャートである。

【図１４】

上記データ伝送システムにおけるデータ伝送の他の手順を示すフローチャートである。

【図１５】

上記データ伝送システムにおけるデータ送信装置側の他の処理手順を示すフロ

ーチャートである。

【図１６】

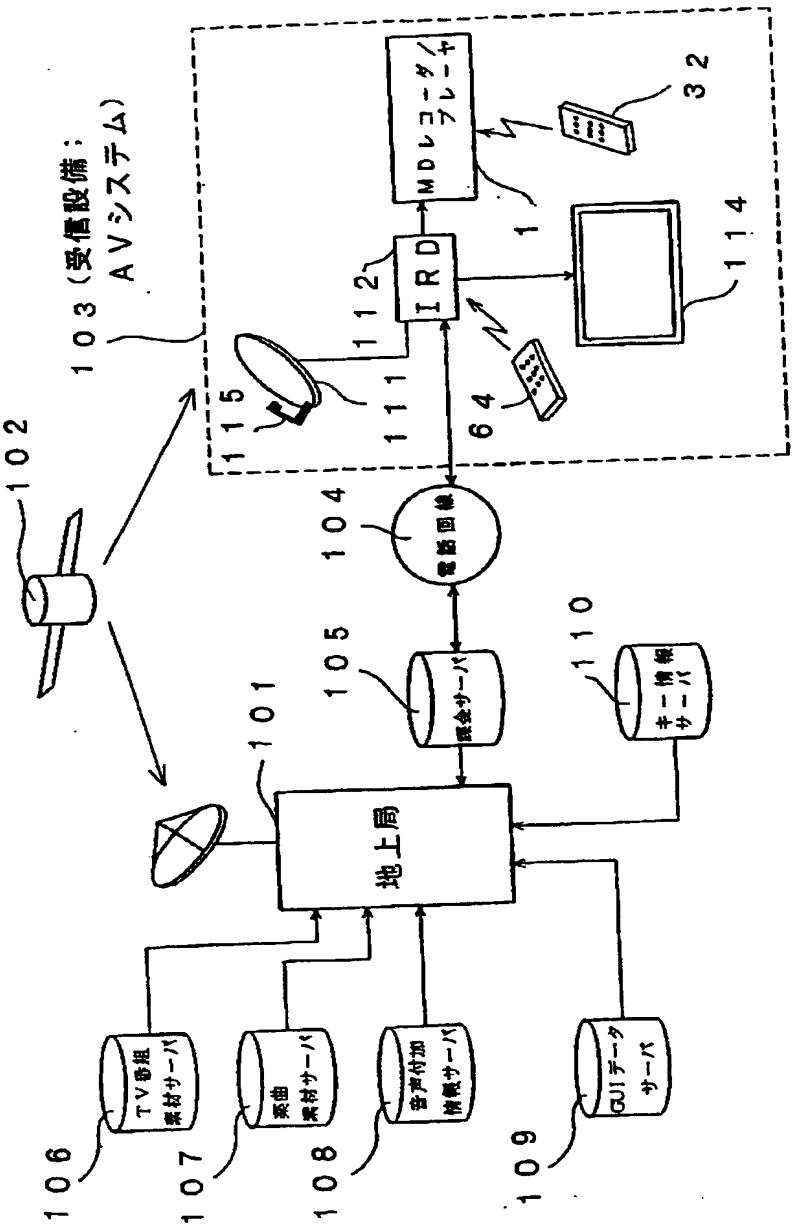
上記データ伝送システムにおけるデータ受信装置側の他の処理手順を示すフローチャートである。

【符号の説明】

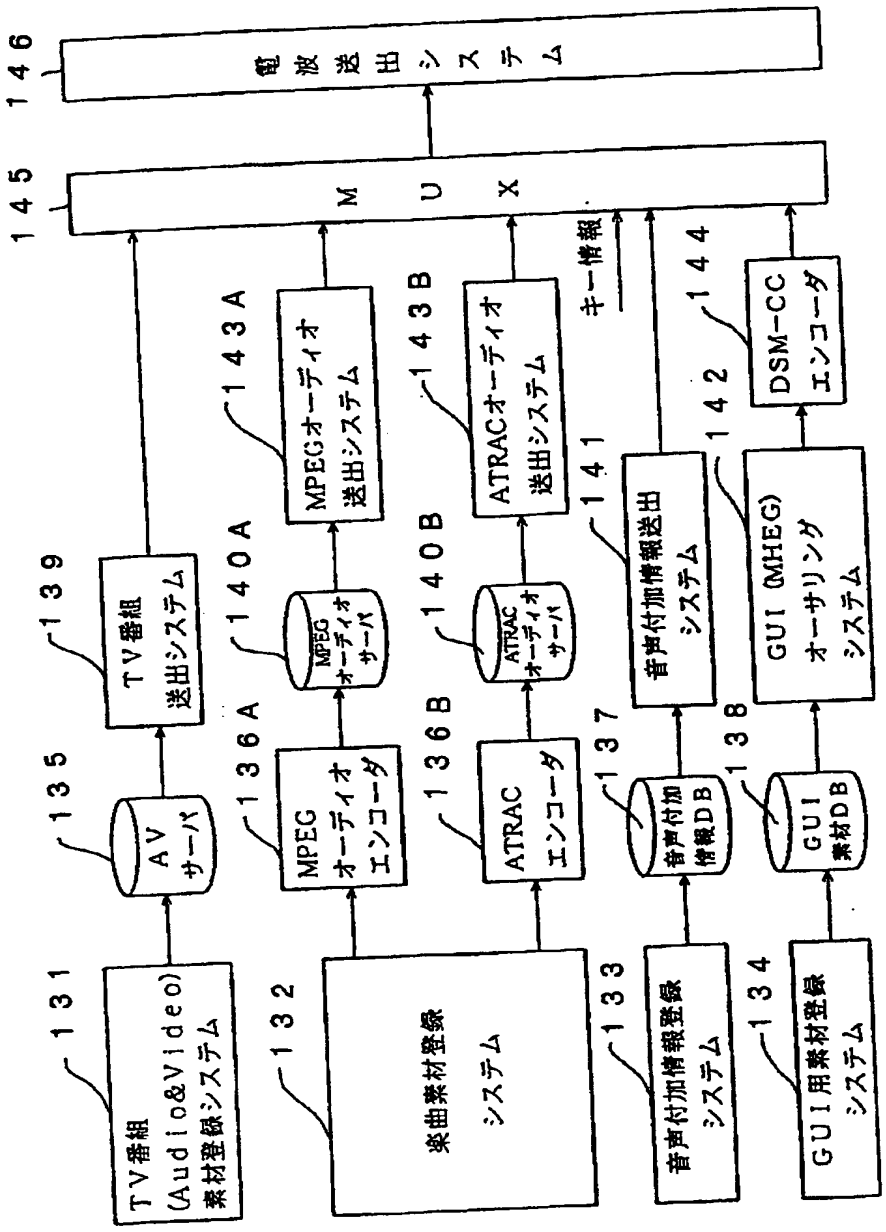
１０　データ送信装置、２０　データ受信装置、３０　伝送路３０、１１，２１　内部バス、１２，２２　ＣＰＵ、１３，２３　メモリ、１４，２４　入力インターフェース、１５，２５　ユーザインターフェース、１６　入出力インターフェース、１８　衛星アンテナ、２６　メディアアクセス部

【書類名】　図面

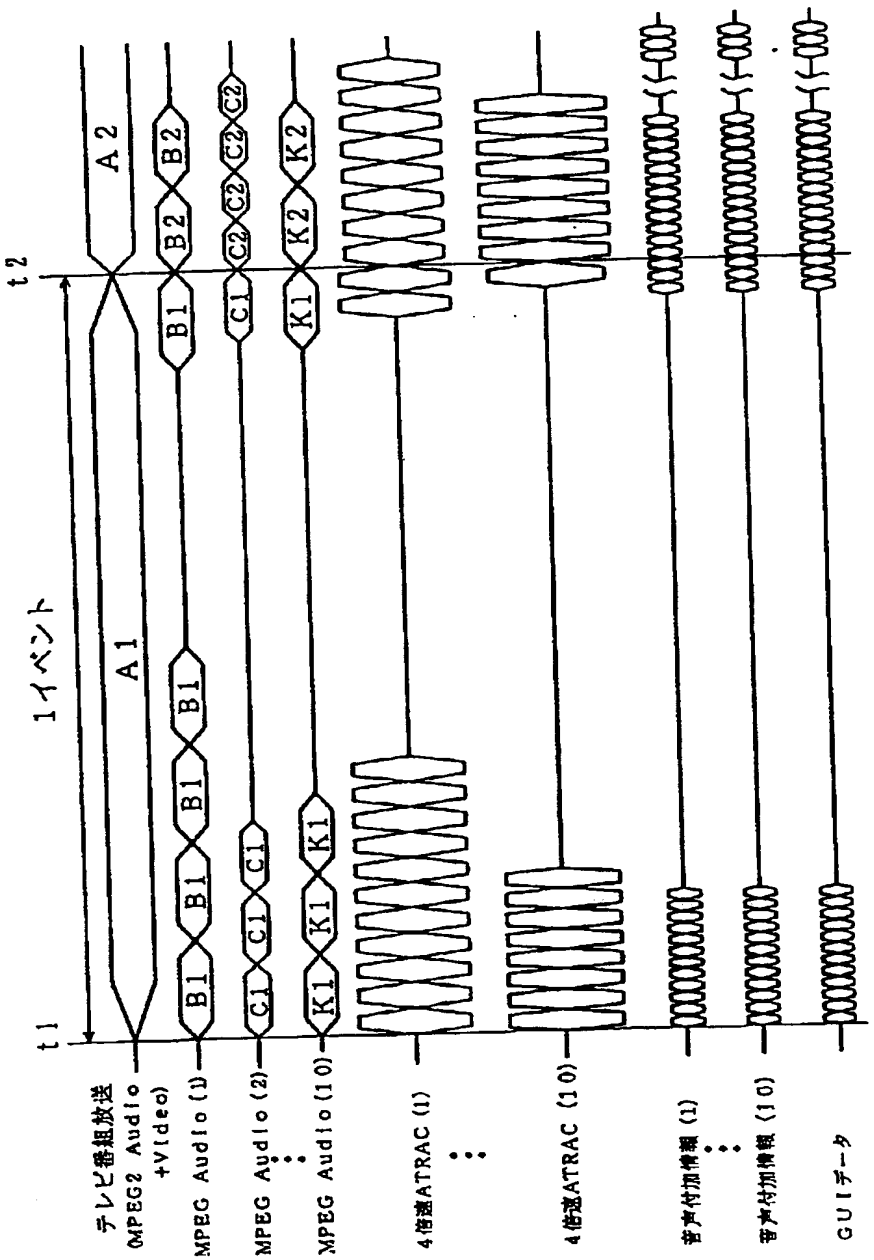
【図１】


103（受信設備：AVシステム）
MDレコーダ/プレーヤ
32
1
IRD
112
114
115
111
64
102
104
電話回線
105
課金サーバ
110
サービス管理サーバ
101
地上局
106
TV番組素材サーバ
107
楽曲素材サーバ
108
音声付加情報サーバ
109
GUIデータサーバ

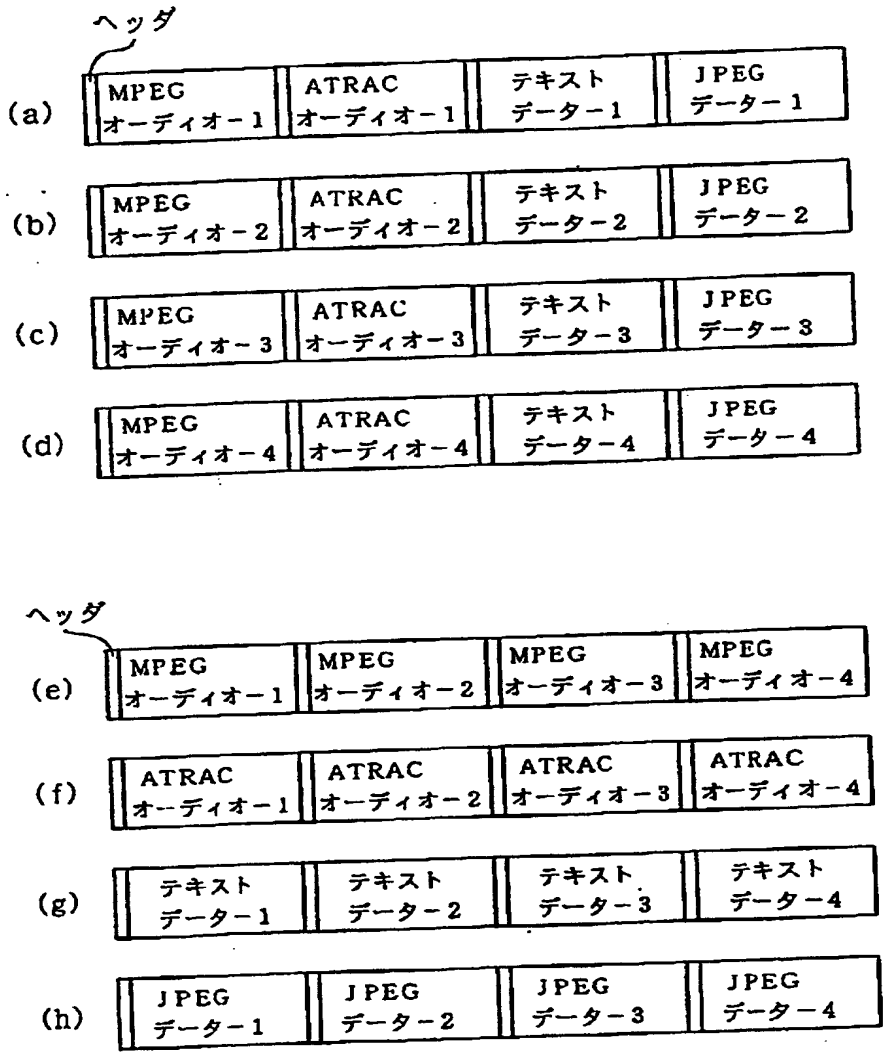
【図２】


１４６
電波送出システム
１４５
MUX
キー情報
１３９
TV番組送出システム
１４０Ａ
MPEGオーディオサーバ
１４３Ａ
MPEGオーディオ送出システム
１４３Ｂ
ATRACオーディオ送出システム
１４０Ｂ
ATRACオーディオサーバ
１４１
音声付加情報送出システム
１４２
GUI (MHEG)オーサリングシステム
１４４
DSM-CCエンコーダ
１３５
AVサーバ
１３６Ａ
MPEGオーディオエンコーダ
１３６Ｂ
ATRACエンコーダ
１３７
音声付加情報DB
１３８
GUI素材DB
１３１
TV番組(Audio&Video)素材登録システム
１３２
楽曲素材登録システム
１３３
音声付加情報登録システム
１３４
GUI用素材登録システム

【図３】

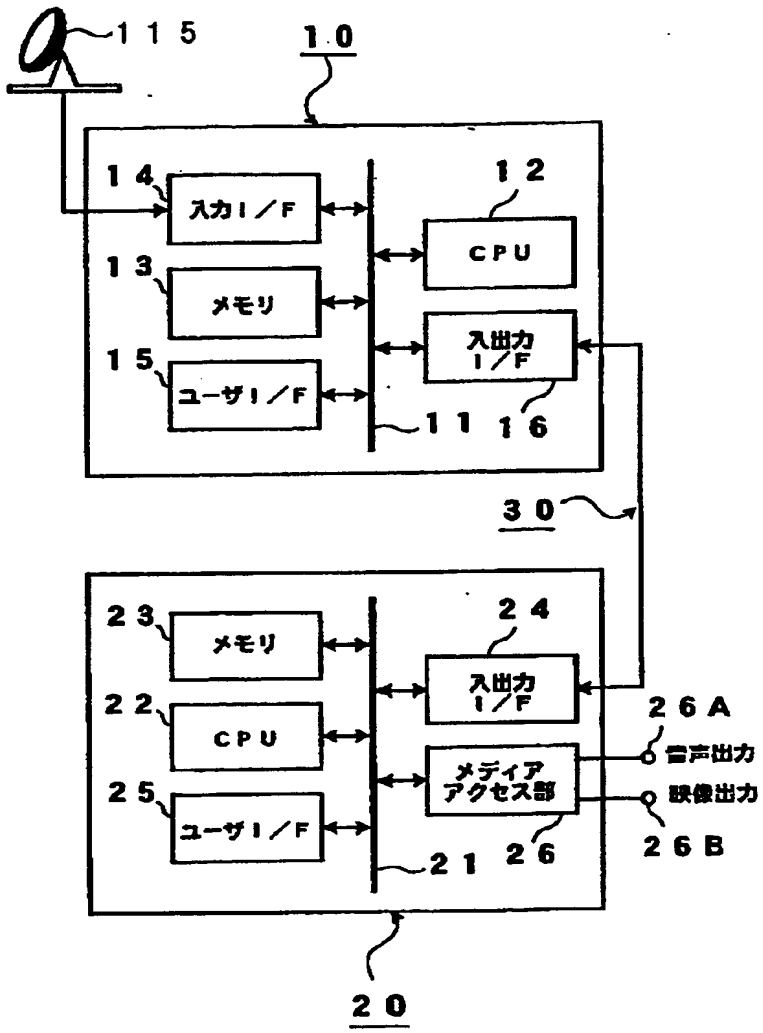

t2
t1
1イベント
A2
A1
B2
B1
C2
C1
K2
K1
テレビ番組放送
MPEG2 Audio
+Video
MPEG Audio (1)
MPEG Audio (2)
MPEG Audio (10)
4倍速ATRAC (1)
4倍速ATRAC (10)
音声付加情報 (1)
音声付加情報 (10)
GUIデータ

【図４】

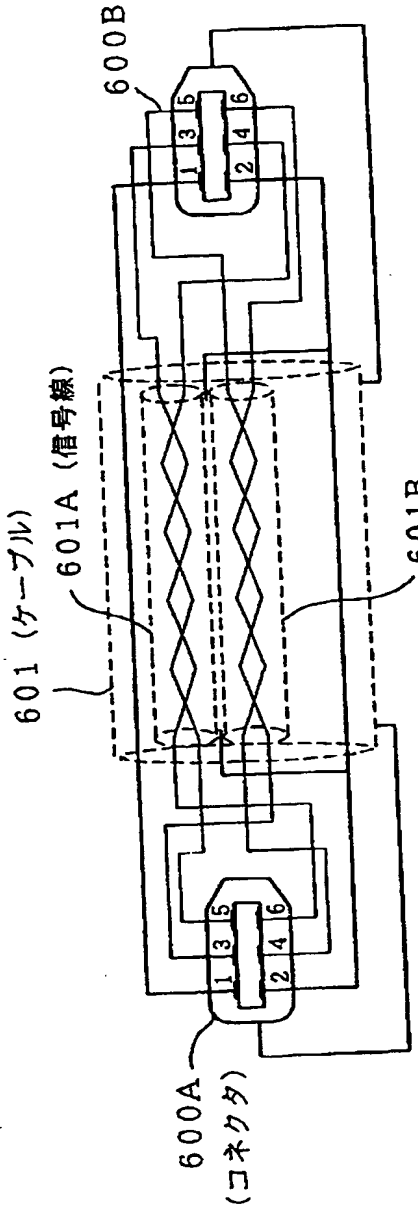


送信側の時分割多重化

【図５】


１１５
１０
１４
入力I／F
１２
CPU
１３
メモリ
入出力
I／F
１５
ユーザI／F
１１
１６
３０
２３
メモリ
２４
入出力
I／F
２６Ａ
２２
CPU
音声出力
メディア
アクセス部
映像出力
２５
ユーザI／F
２１
２６
２６Ｂ
２０

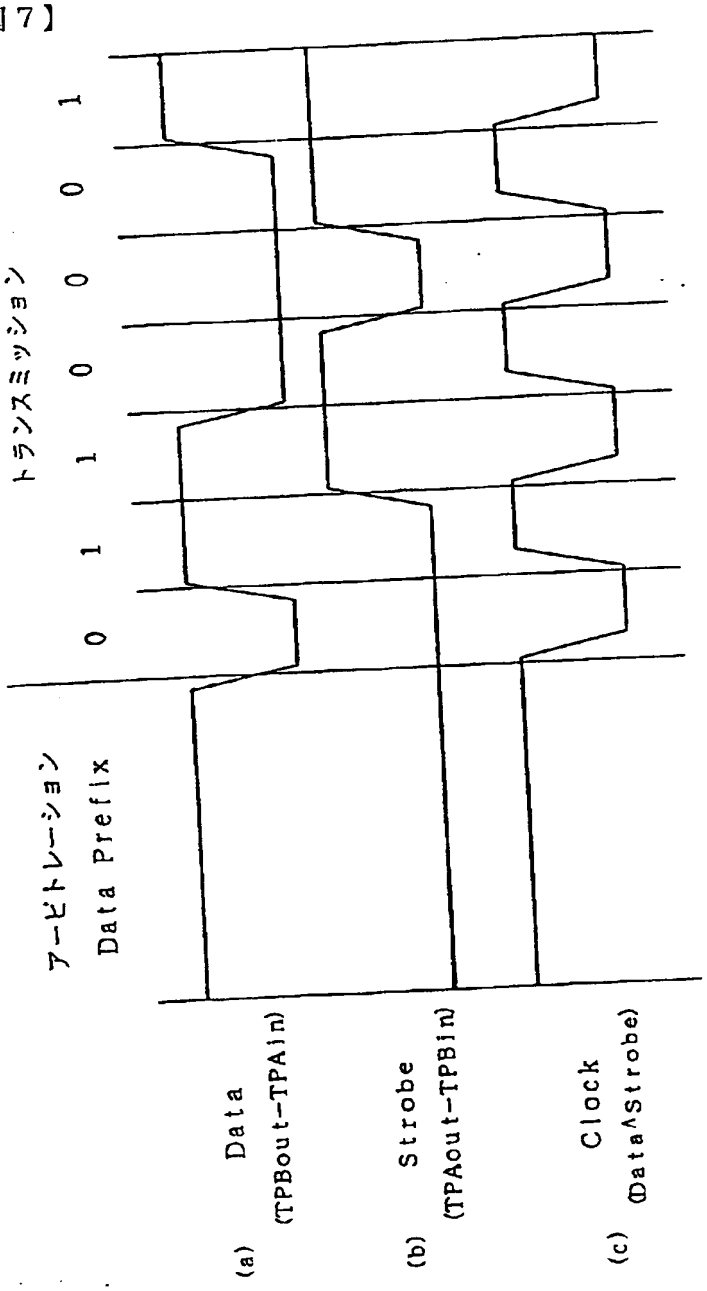
【図６】



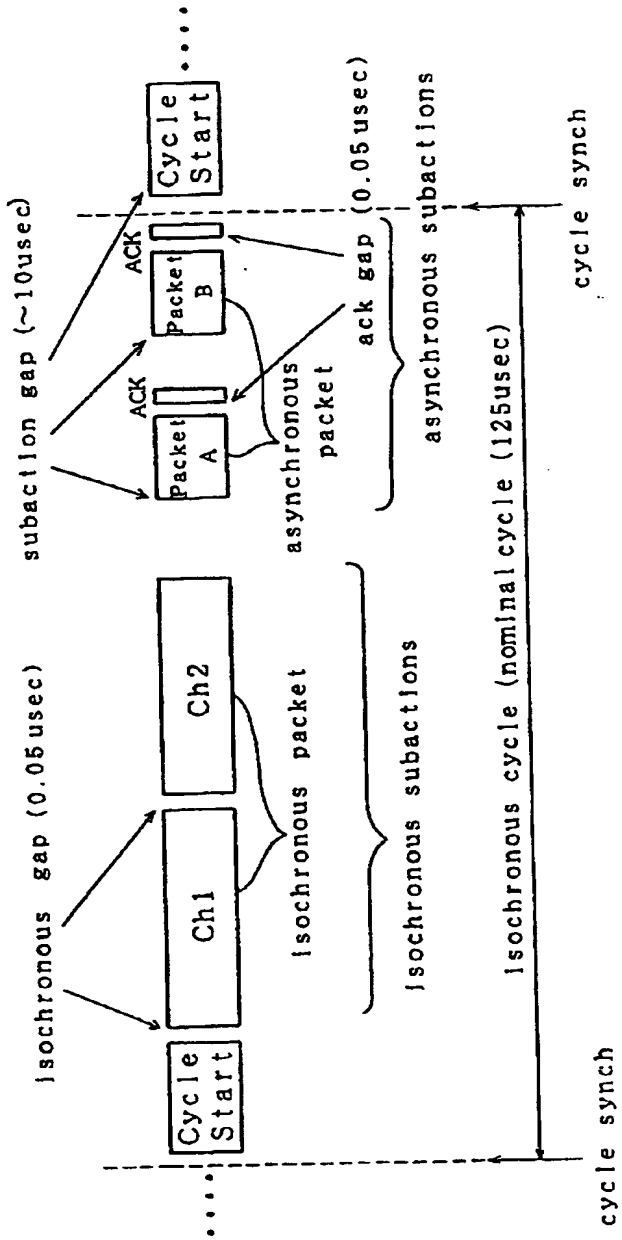
ピン番号	信号
1	VP
2	VG
3	TPB1
4	TPB2
5	TPA1
6	TPA2

ピン番号	信号
1	VP（電源）
2	VG（グランド）
3	TPB1
4	TPB2
5	TPA1
6	TPA2

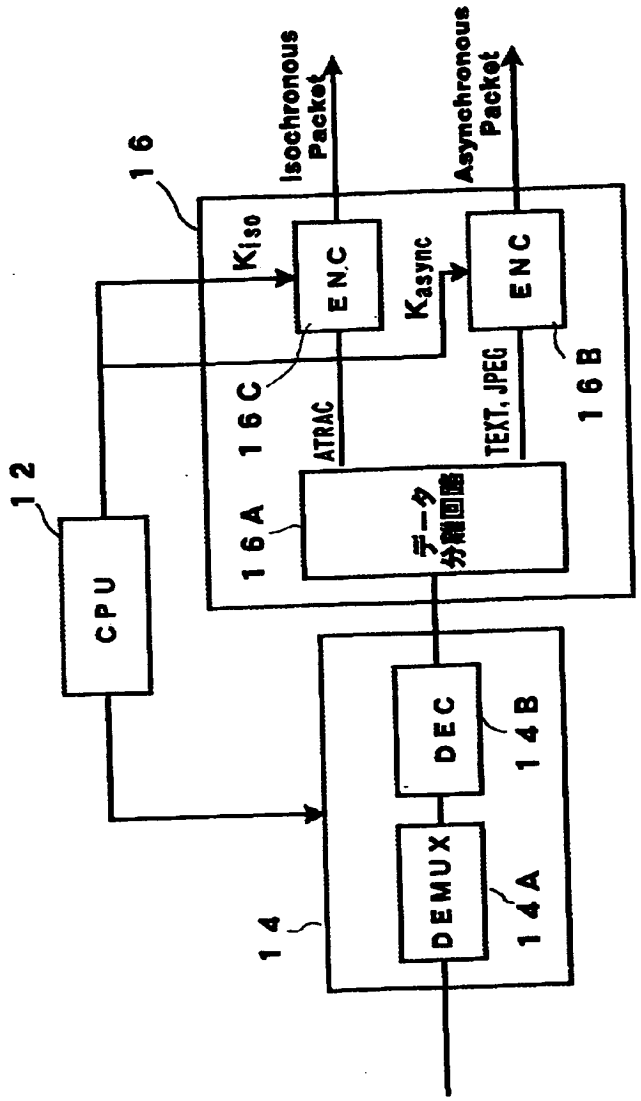
【図７】


アービトレーション
Data Prefix
0
1
1
0
0
0
トランスミッション
1
(a) Data (TPBout-TPAin)
(b) Strobe (TPAout-TPBin)
(c) Clock (Data^Strobe)

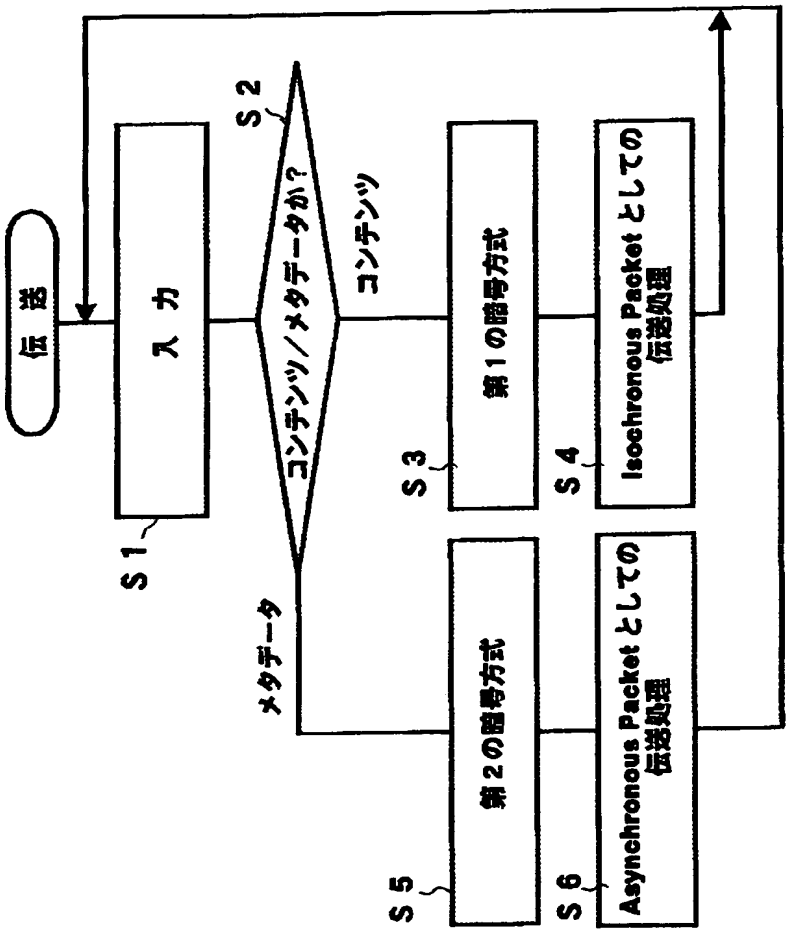
【図８】


Cycle Start
ACK
Packet B
ACK
Packet A
subaction gap (~10usec)
asynchronous packet
ack gap (0.05usec)
asynchronous subactions
cycle synch
Isochronous gap (0.05usec)
Ch1
Ch2
Isochronous packet
Isochronous subactions
Isochronous cycle (nominal cycle (125usec)
Cycle Start
cycle synch

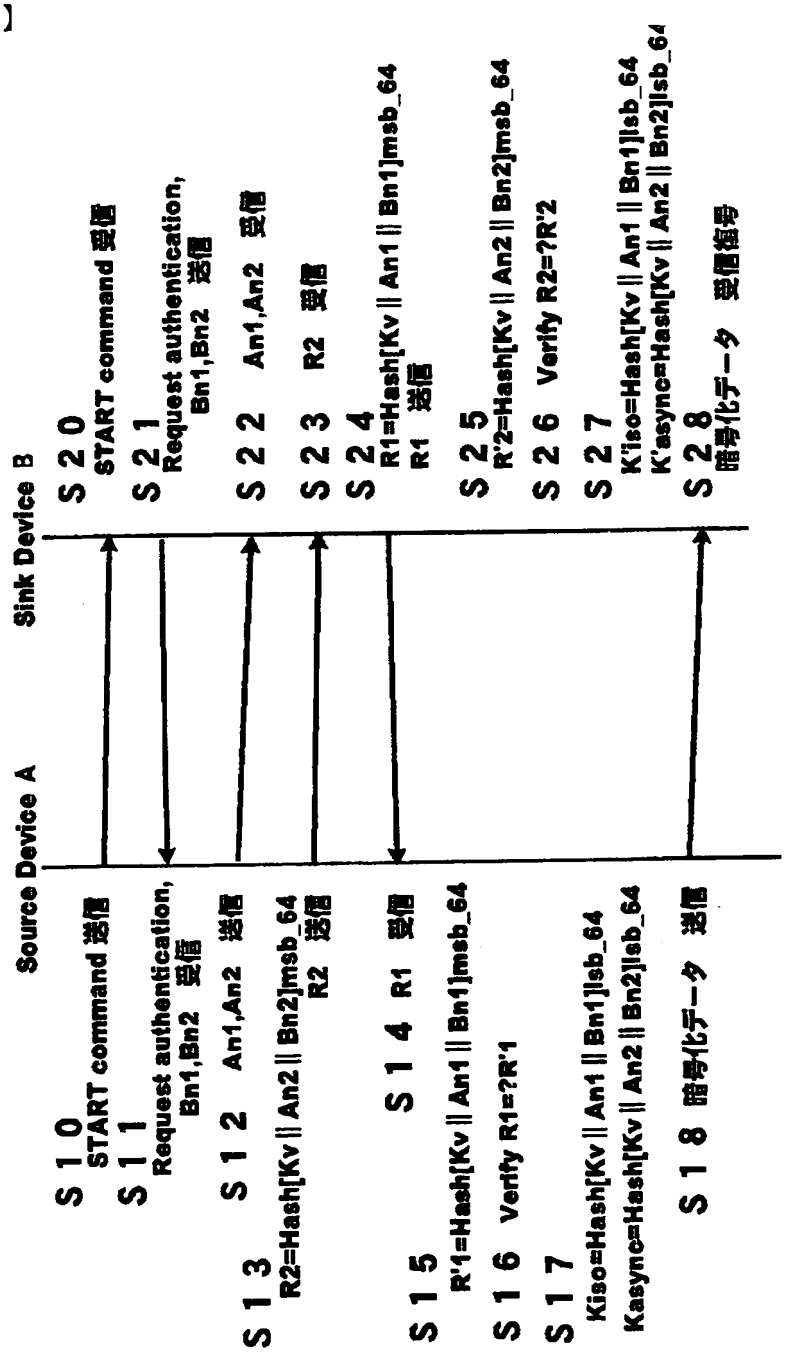
【図９】


Isochronous Packet
Asynchronous Packet
16
Kiso
ENC
Kasync
ENC
16C
ATRAC
TEXT, JPEG
16B
12
16A
データ分離回路
CPU
DEC
14B
DEMUX
14A
14

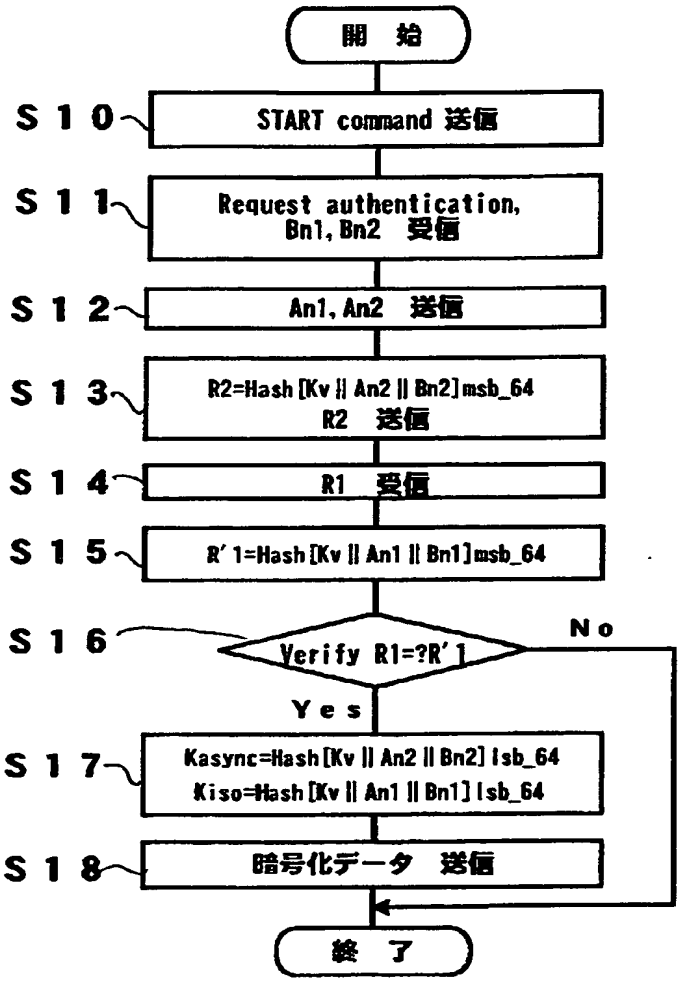
【図１０】


伝送
入力
S1
S2
コンテンツ／メタデータか？
コンテンツ
メタデータ
第１の暗号方式
S3
Isochronous Packet としての伝送処理
S4
第２の暗号方式
S5
Asynchronous Packet としての伝送処理
S6

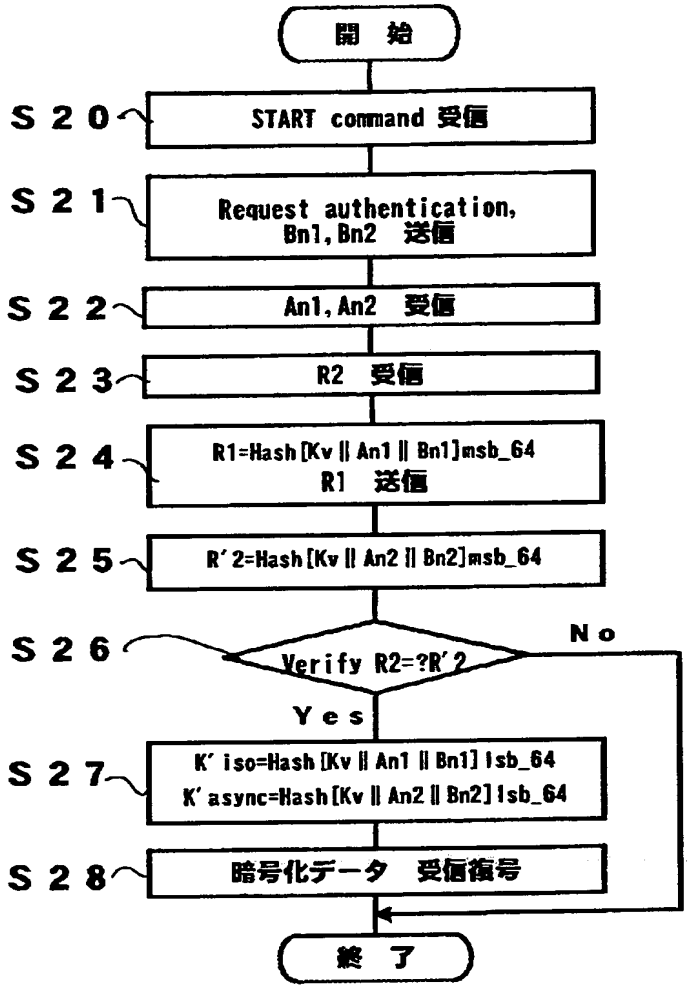
【図１１】


Source Device A
Sink Device B
S10 START command 送信
S11 Request authentication, Bn1,Bn2 受信
S12 An1,An2 送信
S13 R2=Hash[Kv || An2 || Bn2]msb_64 R2 送信
S14 R1 受信
S15 R'1=Hash[Kv || An1 || Bn1]msb_64
S16 Verify R1=?R'1
S17 Kiso=Hash[Kv || An1 || Bn1]lsb_64 Kasync=Hash[Kv || An2 || Bn2]lsb_64
S18 暗号化データ 送信
S20 START command 受信
S21 Request authentication, Bn1,Bn2 送信
S22 An1,An2 受信
S23 R2 受信
S24 R1=Hash[Kv || An1 || Bn1]msb_64 R1 送信
S25 R'2=Hash[Kv || An2 || Bn2]msb_64
S26 Verify R2=?R'2
S27 K'iso=Hash[Kv || An1 || Bn1]lsb_64 K'async=Hash[Kv || An2 || Bn2]lsb_64
S28 暗号化データ 受信復号

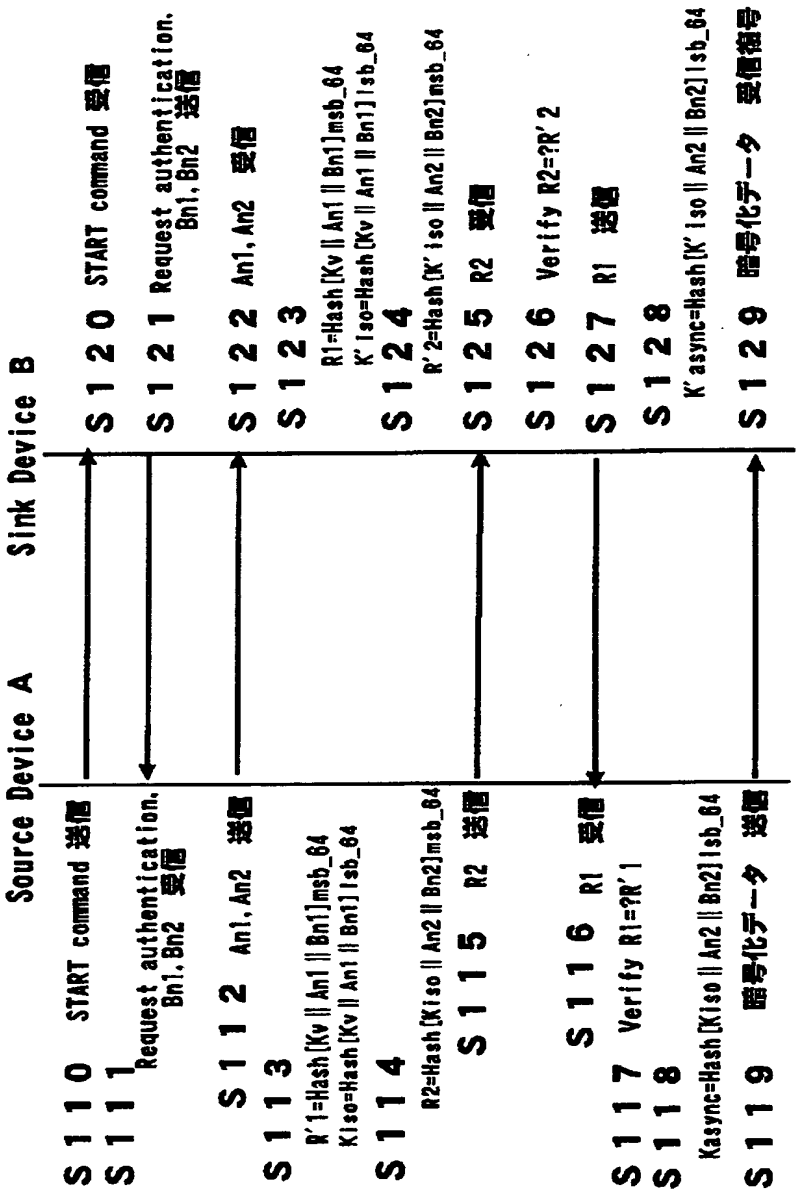
【図１２】


開　始
S１０
START command 送信
S１１
Request authentication,
Bn1, Bn2　受信
S１２
An1, An2　送信
S１３
R2=Hash[Kv || An2 || Bn2]msb_64
R2　送信
S１４
R1　受信
S１５
R'1=Hash[Kv || An1 || Bn1]msb_64
S１６
Verify R1=?R'1
No
Yes
S１７
Kasync=Hash[Kv || An2 || Bn2]lsb_64
Kiso=Hash[Kv || An1 || Bn1]lsb_64
S１８
暗号化データ　送信
終　了

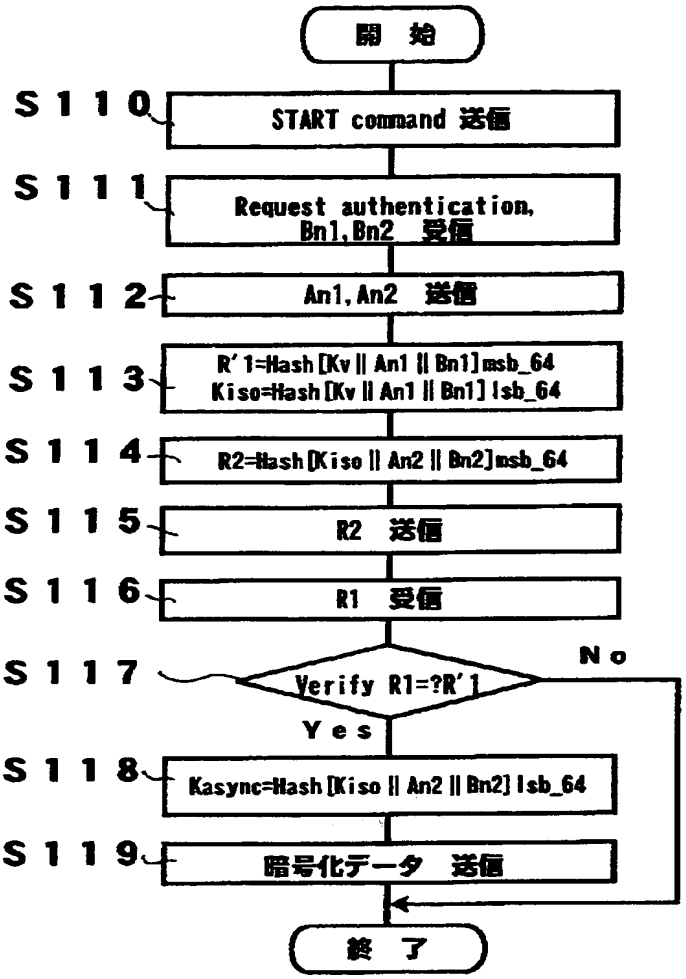
【図１３】


開　始
S20
START command 受信
S21
Request authentication,
Bn1,Bn2　送信
S22
An1,An2　受信
S23
R2　受信
S24
R1=Hash[Kv || An1 || Bn1]msb_64
R1　送信
S25
R'2=Hash[Kv || An2 || Bn2]msb_64
S26
Verify R2=?R'2
No
Yes
S27
K'iso=Hash[Kv || An1 || Bn1]lsb_64
K'async=Hash[Kv || An2 || Bn2]lsb_64
S28
暗号化データ　受信復号
終　了

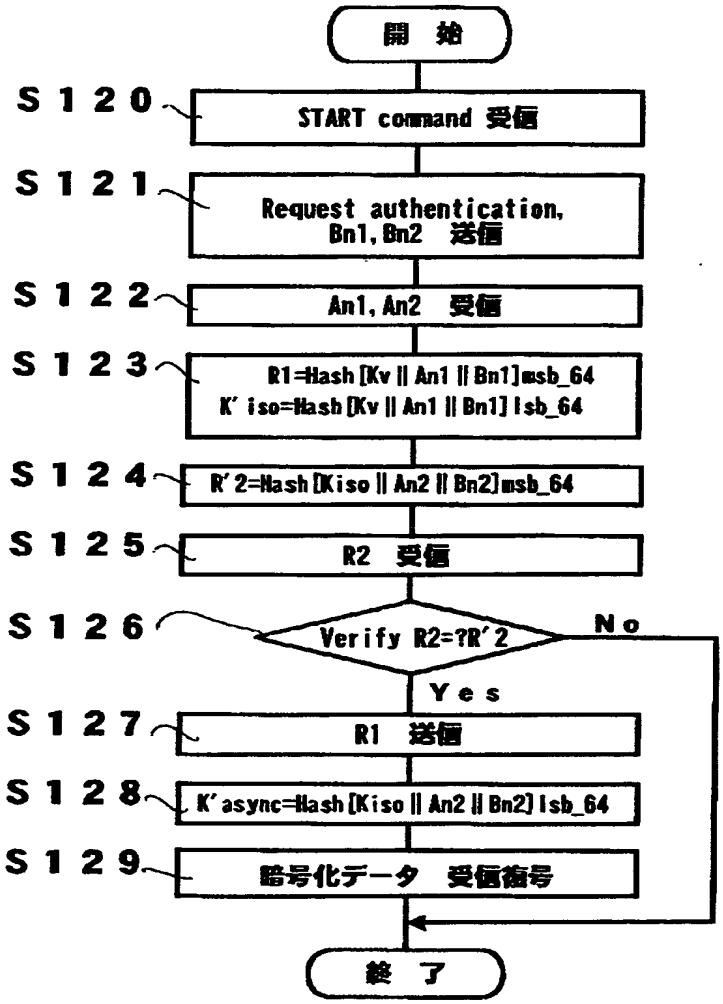
【図１４】


Source Device A
Sink Device B
S110 START command 送信
S111 START command 受信
S112 Request authentication. Bn1, Bn2 送信
S113 Request authentication. Bn1, Bn2 受信
S114 An1, An2 送信
S115 An1, An2 受信
R'1=Hash[Kv || An1 || Bn1]msb_64
Kiso=Hash[Kv || An1 || Bn1]lsb_64
S116
R2=Hash[Kiso || An2 || Bn2]msb_64
S117 R2 送信
S118 R2 受信
S119 Verify R1=?R'1
Kasync=Hash[Kiso || An2 || Bn2]lsb_64
S120 R1 送信
S121 R1 受信
S122 暗号化データ 送信
S123 暗号化データ 受信確認
R1=Hash[Kv || An1 || Bn1]msb_64
K'iso=Hash[Kv || An1 || Bn1]lsb_64
S124
R'2=Hash[K'iso || An2 || Bn2]msb_64
S125 R2 受信
S126 Verify R2=?R'2
S127 R1 送信
S128
K'async=Hash[K'iso || An2 || Bn2]lsb_64
S129 暗号化データ 受信確認

【図１５】


開　始
S110
START command 送信
S111
Request authentication, Bn1, Bn2　受信
S112
An1, An2　送信
S113
R'1=Hash[Kv || An1 || Bn1]msb_64
Kiso=Hash[Kv || An1 || Bn1]lsb_64
S114
R2=Hash[Kiso || An2 || Bn2]msb_64
S115
R2　送信
S116
R1　受信
S117
Verify R1=?R'1
No
Yes
S118
Kasync=Hash[Kiso || An2 || Bn2]lsb_64
S119
暗号化データ　送信
終　了

【図１６】


開　始
S１２０
START command 受信
S１２１
Request authentication,
Bn1, Bn2　送信
S１２２
An1, An2　受信
S１２３
R1=Hash[Kv || An1 || Bn1]msb_64
K' iso=Hash[Kv || An1 || Bn1]lsb_64
S１２４
R'2=Hash[Kiso || An2 || Bn2]msb_64
S１２５
R2　受信
S１２６
Verify R2=?R'2
No
Yes
S１２７
R1　送信
S１２８
K'async=Hash[Kiso || An2 || Bn2]lsb_64
S１２９
暗号化データ　受信指令
終　了

【書類名】　　要約書

【要約】

【課題】　伝送帯域が確保された伝送方式と伝送帯域が確保されていない伝送方式の２種類の伝送方式を採用して、データを安全かつ確実に伝送する。

【解決手段】　データ送信装置１０側のＣＰＵ１２とデータ受信装置２０側のＣＰＵ２２と間で、データ伝送に先立って、相互認証及び複数の暗号鍵を共有するためのプロトコルを実行する。データ送信装置１０は、伝送帯域の保証が必要なデータを上記ＣＰＵ１２により第１の暗号鍵で暗号化して第１の伝送モードで入出力インターフェース１４を介して送信し、上記データに関する関連データを第２の暗号鍵で暗号化して第２の伝送モードで上記入出力インターフェース１４を介して送信し、上記データ受信装置２０は、上記ＣＰＵ２２により、入出力インターフェース２４を介して第１の伝送モードで受信される上記伝送帯域の保証が必要なデータを第１の暗号鍵で復号し、上記入出力インターフェース２４を介して第２の伝送モードで受信される上記関連データを第２の暗号鍵で復号する。

【選択図】　　図５

認定・付加情報

特許出願の番号	平成１１年　特許願　第１４３９８８号
受付番号	５９９００４８８１１２
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１１年　５月２８日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 000002185
- 【住所又は居所】 東京都品川区北品川６丁目７番３５号
- 【氏名又は名称】 ソニー株式会社

【代理人】 申請人
- 【識別番号】 100067736
- 【住所又は居所】 東京都港区虎ノ門２－６－４　第１１森ビル　小池国際特許事務所
- 【氏名又は名称】 小池　晃

【選任した代理人】
- 【識別番号】 100086335
- 【住所又は居所】 東京都港区虎ノ門２丁目６番４号　第１１森ビル　小池国際特許事務所
- 【氏名又は名称】 田村　榮一

【選任した代理人】
- 【識別番号】 100096677
- 【住所又は居所】 東京都港区虎ノ門二丁目６番４号　第１１森ビル　小池国際特許事務所
- 【氏名又は名称】 伊賀　誠司

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社